

**UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO**

CARRERA: INGENIERÍA DE SISTEMAS

**Trabajo de titulación previo a la obtención del título de: INGENIEROS
DE SISTEMAS**

**TEMA:
PROPUESTA DE MEJORAMIENTO DE LA HERRAMIENTA OSSIM SIEM
(OPEN SOURCE), PARA OBTENER LOS NIVELES ÓPTIMOS DE
GESTIÓN EN LA ADMINISTRACIÓN DE LA SEGURIDAD, EN UNA RED
IMPLEMENTADA EN CLOUD COMPUTING**

**AUTORES:
ALEXIS FERNANDO BALAREZO CHÁVEZ
DIEGO XAVIER POVEDA PILATASIG**

**DIRECTOR:
JORGE ENRIQUE LOPÉZ LOGACHO**

Quito, abril de 2015

**DECLARATORIA DE RESPONSABILIDAD Y AUTORIZACIÓN DE USO
DEL TRABAJO DE TITULACIÓN**

Nosotros, autorizamos a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de titulación y su reproducción sin fines de lucro.

Además, declaramos que los conceptos, análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad de los autores.
Quito, abril 2015.

Diego Xavier Poveda Pilatasig
C.C. 172214653-5

Alexis Fernando Balarezo Chávez
C.C. 172231062-8

DEDICATORIA

Al término de mis estudios universitarios, después de todas las horas de trabajo en la elaboración de la tesis de grado dedico la misma a:

Mi madre, Beatriz, un ejemplo de lucha, constancia y mucho sacrificio, gracias a su apoyo y su amor incondicional.

A mis hermanos, Patricia y John, quienes tuvieron que luchar duro a mi lado toda la vida para salir adelante.

A mi sobrino David, que desde que llegó a mi vida se convirtió en una razón para luchar y ser un ejemplo para él.

A mi novia, Karina, gracias por estar a mi lado, por tu apoyo, por entregarme el aliento que necesitaba cuando sentía que no podía más.

Diego Xavier Poveda Pilatasig

A mi familia por el apoyo brindado en cada uno de los pasos dados en el transcurso de la carrera, siendo ellos el motivo por el cual se ha luchado por subir un peldaño más en la vida profesional.

A mi padre y a mi madre por el sacrificio realizado por y para mí al respaldar una de las decisiones más importantes de mi vida de principio a fin.

A mis hermanas y sobrinos que estuvieron ahí en los momentos difíciles para levantarme e impulsarme de una u otra forma para salir adelante.

A todos quienes estuvieron y están a mi lado dándome apoyo moral para no rendirme a pesar de las adversidades del camino de la existencia.

Alexis Fernando Balarezo Chávez

AGRADECIMIENTO

A la Universidad Politécnica Salesiana por aportar con todo lo que necesitábamos en el desarrollo de la tesis de grado.

Un eterno agradecimiento al Ingeniero Jorge López quien aportó con sus conocimientos y su experiencia en la elaboración y culminación del presente trabajo de grado.

ÍNDICE

INTRODUCCIÓN	1
CAPÍTULO 1.....	2
MARCO TEÓRICO	2
1.1 Planteamiento del problema.....	2
1.2 Objetivos	3
1.2.1 Objetivo general	3
1.2.2 Objetivos específicos	3
1.3 Justificación.....	3
1.4 Marco Teórico.....	5
1.4.1 Seguridad Informática.....	5
1.4.2 Objetivos de la seguridad informática.....	6
1.4.3 Medidas de la seguridad informática	7
1.4.4 Amenazas a la información.....	8
1.4.5 Amenazas a la seguridad de la información.....	9
1.4.6 Elementos considerados amenazas	9
1.4.7 Estándares de autenticación de usuarios PCI e ISO.....	11
1.4.8 Arreglo RAID.....	15
1.4.9 Cloud Computing.....	16
1.4.10 OSSIM.	20
CAPÍTULO 2.....	27
DISEÑO E IMPLEMETACIÓN	27
2.1 Fase de preparación.....	27
2.2 Fase de planificación.....	29
2.3 Fase de diseño	30
2.3.1 Servidor RAID	30
2.3.2 Servidor Cloud Computing	31
2.3.3 Sistema OSSIM.....	32
2.4 Fase de implementación.....	34
2.4.1 Instalación Cloud Computing	34
2.4.2 Instalación OSSIM.....	37
2.5 Fase de operación.....	38

2.5.1 Análisis funcional Cloud Computing.....	38
2.5.2 Análisis funcional OSSIM	41
2.6 Fase de optimización.....	41
CAPÍTULO 3.....	42
PRUEBAS, DESARROLLO E INTEGRACIÓN	42
3.1 Pruebas	42
3.1.1 Herramientas de OSSIM.	42
3.2 Desarrollo.....	48
3.2.1 Soluciones de tiempos de respuesta en OSSEC.....	49
3.2.2 Gestor de integración de datos para NAGIOS	55
CAPÍTULO 4.....	60
PRUEBAS.....	60
4.1 Pruebas funcionales Cloud Computing.....	60
4.2 Pruebas funcionales NAGIOS	65
4.3 Pruebas funcionales OSSEC	69
CONCLUSIONES.....	73
RECOMENDACIONES.....	75
LISTA DE REFERENCIAS	76
GLOSARIO DE TÉRMINOS.....	77
ANEXOS	79

ÍNDICE TABLAS

Tabla 1. <i>Característica principal de los objetivos de la seguridad informática</i>	6
Tabla 2. <i>Amenazas según el propósito de afectación</i>	9
Tabla 3. <i>Artículos referentes al monitoreo del acceso y el uso del sistema</i>	15
Tabla 4. <i>Arquitectura de los sistemas RAID</i>	15
Tabla 5. <i>Niveles de RAID utilizados a nivel empresarial, home</i>	16
Tabla 6. <i>Descripción de las ventajas y desventajas de la Cloud Computing</i>	19
Tabla 7. <i>Partes que constituyen a OSSIM</i>	20
Tabla 8. <i>Formas de instalación de la herramienta OSSEC</i>	23
Tabla 9. <i>Estado de puertos en la lista de información de NMAP</i>	23
Tabla 10. <i>Descripción y funcionalidades de elementos de arquitectura de OSSIM</i> ..	26
Tabla 11. <i>Elementos de una red</i>	28
Tabla 12. <i>Estructura de una red</i>	28
Tabla 13. <i>Requerimientos para el diseño del Laboratorio</i>	29
Tabla 14. <i>Funcionalidades XenServer 6.5 (Free)</i>	38
Tabla 15. <i>Descripción de las soluciones</i>	49
Tabla 16. <i>Pruebas de funcionalidad de la Cloud Computing (XenServer)</i>	60
Tabla 17. <i>Abreviaturas para la prueba de funcionalidad de la Cloud Computing</i> . ..	61
Tabla 18. <i>Resultados obtenidos, nodo 1</i>	62
Tabla 19. <i>Resultados obtenidos, nodo 2</i>	63
Tabla 20. <i>Resultados obtenidos, nodo máster</i>	64
Tabla 21. <i>Pruebas de funcionalidad Generador de host NAGIOS</i>	65
Tabla 22. <i>Promedio de configuración</i>	67
Tabla 23. <i>Resultados obtenidos</i>	69
Tabla 24. <i>Medición de tiempos de respuesta generación-visualización eventos</i>	70
Tabla 25. <i>Promedio comparativo de tiempos pre-post implementación</i>	71
Tabla 26. <i>Optimización de tiempos de respuesta por host</i>	71

ÍNDICE FIGURAS

<i>Figura 1.</i> Ilustración objetivos en la seguridad informática	7
<i>Figura 2.</i> Tipo de amenazas.....	9
<i>Figura 3.</i> Tipos de ataques a la seguridad informática	10
<i>Figura 4.</i> Arquitectura Cloud Computing.....	18
<i>Figura 5.</i> Arquitectura por capas de OSSIM	22
<i>Figura 6.</i> Metodología PPDIOO para diseño de Laboratorio.....	27
<i>Figura 7.</i> Cálculo matemático funcionamiento RAID 5.....	31
<i>Figura 8.</i> Diagrama del laboratorio de pruebas	33
<i>Figura 9.</i> Arquitectura de la herramienta XenServer.....	34
<i>Figura 10.</i> Funcionamiento CITRIX XenServer	40
<i>Figura 11.</i> Panel de visualización, muestra la información obtenida por OSSEC	42
<i>Figura 12.</i> Evento OSSEC de adición de archivo en directorio	44
<i>Figura 13.</i> Escaneo de activos de red mediante herramienta NMAP	45
<i>Figura 14.</i> Listado de activos descubiertos mediante escaneo NMAP.....	45
<i>Figura 15.</i> Consola administrativa NAGIOS equipos agregados manualmente	48
<i>Figura 16.</i> Modelo de desarrollo iterativo e incremental	49
<i>Figura 17.</i> Muestra las reglas creadas para la autenticación de los usuarios.....	54
<i>Figura 18.</i> Sensores de consumo CPU y Memoria.....	61
<i>Figura 19.</i> Valores de conmutación de la VM del nodo1	62
<i>Figura 20.</i> Valores de conmutación de la VM del nodo1 y nodo2.....	63
<i>Figura 21.</i> Valores correspondientes al inicio y final de la prueba XenServer	64
<i>Figura 22.</i> Estadísticas de tiempos de configuración para NAGIOS	68
<i>Figura 23.</i> Generación de eventos mediante autenticación ssh errónea y acertada...	69
<i>Figura 24.</i> Tiempo promedio de visualización de eventos autenticación correcto....	72
<i>Figura 25.</i> Tiempo promedio de visualización de eventos autenticación erróneo	72

ÍNDICE ANEXOS

Anexo 1. Configuración RAID 5	79
Anexo 2. Configuración Cloud Computing	81
Anexo 3. Accesos máquinas virtuales.....	87
Anexo 4. Gestor de host NAGIOS	89
Anexo 5. Pruebas OSSEC optimización de tiempos.....	92

RESUMEN

La presente investigación trata sobre la optimización de un sistema OSSIM, el cual se implementó en la Cloud Computing, tecnología en crecimiento a nivel empresarial, motivo por el cual se busca integrar un sistema de monitoreo que preste confiabilidad a la red y sus activos. Existiendo múltiples sistemas para el montaje de la Cloud, en el presente trabajo se usó la plataforma CITRIX XenServer por tratarse de sistema Open Source.

Teniendo en cuenta dos características importantes de la Cloud que son la accesibilidad y la estabilidad, se ha implementado mediante software un servidor RAID5 para generar un dispositivo lógico de almacenamiento y se configuro la alta disponibilidad con el que cuenta la plataforma de la nube, certificando inexistencia de pérdidas.

Indagando en los requerimientos empresariales el punto en común que poseen, es el costo, en su mayoría buscan optimizar seguridad a bajo costo por lo cual se hizo uso del sistema AlienVault OSSIM siendo este de código abierto basado en el Kernel de Debian. El sistema cubre muchas expectativas al tratarse de una plataforma que administra varias herramientas de monitoreo unificadamente.

Entre las herramientas tratadas se encuentran el detector OSSEC, teniendo un funcionamiento basado en logs generados por los equipos que forman parte de la red, los monitores NMAP y NAGIOS los cuales funcionan basados en respuestas a solicitudes realizadas por estas herramientas.

Las funcionalidades de NMAP junto a comandos útiles de terminal permitieron optimizar la gestión de host para NAGIOS automatizando el registro de cada uno mediante un script.

ABSTRACT

The investigation is about the OSSIM system optimization, this system is implemented on the Cloud Computing, in the enterprise world has increased this technology and this is the reason because seeks to integrate a monitor system that provide reliability in the network and your connected assets. In the environment exist some systems for assemble a Cloud Computing, in this work has used CITRIX XenServer platform because it's an Open Source system.

Considering that two of characteristics of Cloud are the accessibility and the stability, has been implemented through software a RAID 5 server for generate a storage logical device and configure the high availability system is attached in the Cloud Computing platform, this certifies inexistence of services losses or information losses.

Investigating into enterprise requirements one of common themes they have is the cost, mostly looking for security optimization with low cost so it was used AlienVault OSSIM system which is open source, based in Debian kernel. The system meets some expectations because it's a platform that manages several monitoring tools unitedly.

Among the tools used are the OSSEC detector, that works based in generated logs by the equipments connected in the network, the monitors NMAP and NAGIOS that their works based in responses requests that been generated this tools.

The joint work of NMAP tool and helpful terminal commands have allowed optimize the host management for NAGIOS tool with the automatic register for each connected host on the network that was done by creating a assets information generator script.

INTRODUCCIÓN

En la actualidad las organizaciones se desarrollan significativamente e invierte una gran cantidad de recursos económicos en la adquisición de herramientas licenciadas, que en la mayoría de casos no cumplen con la expectativa de la entidad y las cuales no pueden adaptarse a cambios en su funcionalidad.

La principal meta del Software Libre es llevar el modelo de desarrollo Open Source al mundo empresarial, la principal ventaja y la más obvia de estos sistemas es la no existencia de un costo monetario en licencias para un determinado producto, esto se lleva a cabo gracias a la disponibilidad del código fuente que brinda una determinada independencia al proveedor, el cual es considerado como el contribuyente original del sistema. Al disponer del código fuente se puede ajustar el producto y mejorarlo para cubrir las necesidades de cualquier organización, en el área de la seguridad la posibilidad de modificación del código fuente es indispensable ya que el número ataques y amenazas son cada vez más complejas de identificar y toma más tiempo buscar una solución.

Este proyecto está enfocado al mejoramiento de la herramienta OSSIM de AlienVault, que al poseer las funcionalidades de un SIEM, permitiendo integrar la información en tiempo real de varios sistemas de monitoreo y detección de anomalías en una red de servicios, como es la Cloud Computing, la expectativa a cumplirse es la de proporcionar las mejoras necesarias al sistemas OSSIM y obtener una visibilidad de todos los eventos que se presentan en la nube aumentando los tiempo de configuración y gestión de la información por parte del administrador.

CAPÍTULO 1

MARCO TEÓRICO

1.1 Planteamiento del problema

El inconveniente más grande que presenta una empresa al momento de gestionar la información es la seguridad de los datos, pues la mayoría de los usuarios tienen que seguir ciertos protocolos de seguridad, pero estos no son utilizados de manera correcta a pesar de que son sencillos de utilizar, por otra parte, son muy fáciles de atacar; un ejemplo de este problema es la contraseña simple que pueden ser utilizada para acceder a una gran cantidad de datos y aplicativos en una empresa, este comportamiento erróneo de un usuario, permite que los atacantes intenten descifrar dichas contraseñas utilizando distintos métodos para obtener el acceso a la información.

Para evitar este tipo de problemas las empresas optan por utilizar herramientas de seguridad sumamente costosas, lo que hace que la empresa se vuelva dependiente del proveedor al momento de presentarse un nuevo ataque, el empresario tendrá que adquirir más licenciamiento o en el peor de los casos, una nueva herramienta para repeler estos ataques. En la actualidad existen una gran variedad de software de código abierto el cual puede ser mejorado, modificado e incluso actualizado desde su propio Kernel, para que así, dependiendo del ataque, el software sea acoplado para obtener la información necesaria y bloquear los ataques sin que esto represente una inversión adicional a la empresa. A medida que estas aplicaciones se van desarrollando es necesaria más información para poder identificar el ataque, por este motivo es necesario que el administrador de las herramientas de seguridad de la información este siempre en constante actualización y preparación.

Por otra parte, las empresas no están seguras de utilizar herramientas de código abierto ya que se tienen la mentalidad de que todo lo barato en este caso sin costo sale caro, al momento las herramientas de código abierto presentan una gran cantidad de falencias, pero dichos errores pueden ser corregidos y adaptados para cada necesidad al momento de implementar la seguridad informática en la gestión de los servicios y la información.

1.2 Objetivos

1.2.1 Objetivo general

Mejorar la función de la herramienta OSSIM SIEM, para obtener los niveles óptimos de gestión en la administración de la seguridad en una red basada en Cloud Computing.

1.2.2 Objetivos específicos

Sistematizar los conceptos basados en el Cloud Computing como son: creación, monitoreo y seguridades existentes en las redes mediante el uso de las herramientas OpenStack y XCP.

- Implementar una nube con el uso de las herramientas OPENSTACK y XCP a través de la construcción de un arreglo redundante de discos independientes RAID.
- Implementar un laboratorio de pruebas en la CLOUD COMPUTING que permita integrar la herramienta OSSIM y los dispositivos de simulación de una red.
- Analizar los sucesos obtenidos de la herramienta OSSIM en el monitoreo de la red acoplada en la nube, para solventar las brechas de seguridad de la misma.
- Modificar el código fuente de la herramienta OSSIM para mejora de funcionamiento y su posterior análisis y creación de reglas de seguridad basadas en los estándares PCI e ISO en la autenticación de usuarios para bloquear ataques a la red con mayor precisión.

1.3 Justificación

En la actualidad la seguridad informática es una disciplina, que se encarga de proteger la información almacenada en un sistema informático distribuido en su totalidad en las redes de datos, todavía, no se tiene un sistema en su totalidad seguro, que sea capaz de brindar la integridad y privacidad de la información en un cien por ciento.

La posibilidad de interconectarse a través de grandes redes es el punto clave para que las empresas inviertan en mejores alternativas para la protección de la información; mientras las empresas buscan nuevas formas de combatir los nuevos ataques

informáticos, al mismo tiempo, nuevas amenazas se desarrollan, por este motivo, dichas empresas invierten miles de dólares para la anulación de los ataques.

En la actualidad la utilización de software no propietario es la opción más óptima para la seguridad de la información, ya que, al ser código abierto se lo puede ir mejorando dependiendo de la necesidad y así mejorar el sistema de protección a un bajo costo.

La seguridad informática en las redes de datos se la puede clasificar en seguridad lógica y física, las cuales buscan con la ayuda de políticas de control mantener la seguridad de los recursos y la información. En el nivel físico se puede considerar como importante a los firewall, los cuales, permiten el control del acceso de cada host. A nivel lógico existe variedad de herramientas licenciadas, las cuales permiten realizar un control de acceso más minucioso para cada host, al utilizar herramientas libres y modificables se puede cambiar los parámetros del sistema para que se pueda acoplar a las reglas de cada acceso.

En la actualidad, una de las herramientas usadas por los administradores de red que les permite realizar cambios para su rendimiento es OSSIM (Open Source Security Information Management), la cual está basada en la captura de eventos producidos mediante el paso de tráfico en la red, dicha herramienta es la encargada de identificar las vulnerabilidades de la red de datos por medio de la recolección de información, permitiendo así, generar reglas y políticas de acceso, haciendo de ésta una parte importante para el uso adecuado de los recursos, de red mediante la alerta de ataques que producen alguna anomalía, la cual no es identificada por las herramientas IDS tradicionales.

OSSIM a pesar de ser una herramienta usada constantemente para la seguridad de las redes, tiene algunas falencias como el trabajo conjunto con el sistema de monitoreo de redes de datos NAGIOS, el cual hace su trabajo, pero no identifica y configura los equipos en la consola de forma automática y con esto reducir los tiempo en la administración de la red. (Martinez, 2013).

La utilización de herramientas Open Source es la opción óptima al momento de proteger la información en la red, ya que la principal razón para que una empresa utilice la herramienta es la reducción de costos, al hablar de reducción de costos es importante que se piense en migrar toda la información a un mejor sistema, como lo es la nube informática, pues no se tendría inconvenientes a nivel físico ni una limitación en el almacenamiento, como sucede actualmente.

Se piensa, que es un gran error migrar la información a la Cloud que es un medio de almacenamiento y transporte de información, pero el gran error es no hacerlo, dado que esto evitará que la información sea almacenada en dispositivos físicos de la propia empresa o dispositivos personales, los cuales puedan presentar algún problema lógico o físico, que afecte la información. Gracias al mejoramiento de las herramientas de software libre, se está logrando que la información que se encuentran en la nube sea y se mantenga lo más segura al momento de utilizarla.

1.4 Marco Teórico

1.4.1 Seguridad Informática

La seguridad informática, se encarga de minimizar los riesgos asociados con el acceso y utilización de los sistemas de forma malintencionada, esto implica, que se debe tener una visión general de los bienes a los cuales se necesita proteger, los cuales deben ser analizados para poder reducir al mínimo los riesgos, con esto se logra tener un control en la utilización de medidas preventivas y correctivas en la seguridad.

Se considera que en la informática el análisis de los riesgos es complejo por la cantidad de información y el alto número de eventos potenciales, esto conlleva a que se tenga una gran cantidad de medidas de seguridad, las cuales al momento de utilizarlas dificulta su elección, sin embargo estas medidas servirán para proteger un bien de un conjunto de riesgos.

Al momento del diseño de un sistema informático se debe considerar que la seguridad es una parte fundamental, es la única medida que garantiza que la información utilizada en el sistema no sufra algún tipo de acceso inadecuado e indebido por terceras personas.

1.4.2 Objetivos de la seguridad informática

La seguridad informática implica un conjunto de procedimientos estratégicos que permiten gestionar los tres principios fundamentales de la seguridad tales como la integridad, disponibilidad y la confidencialidad de la información a la que se tiene acceso, que son los objetivos principales de la seguridad.

- **Integridad**

Los accesos fraudulentos a la información ocasionan que se genere una gran cantidad de robos informáticos como por ejemplo una transacción bancaria, al permitir que la información sea capturada y modificada puede dar paso a procesos erróneos en un organización y producir el desbordamiento de otros ataques.

- **Disponibilidad**

La información deber estar disponible en todo momento y responder en un tiempo estipulado, caso contrario, produce una perdida en la credibilidad de la entidad que maneja la información.

- **Confidencialidad**

La información no será difundida por ningún motivo no autorizado, si se llegara a perder la confidencialidad produciría problemas legales y se podría perder la credibilidad de la organización e incluso se puede llegar a la caída total del negocio.

Tabla 1. *Característica principal de los objetivos de la seguridad informática*

Objetivos	Descripción
Integridad	La información no será alterada por personal no autorizado.
Disponibilidad	Información disponible en todo momento.
Confidencialidad	Información no será difundida.

Nota. Objetivos de la seguridad informática
Elaborado por: Diego Poveda & Alexis Balarezo

Objetivos en la seguridad informática

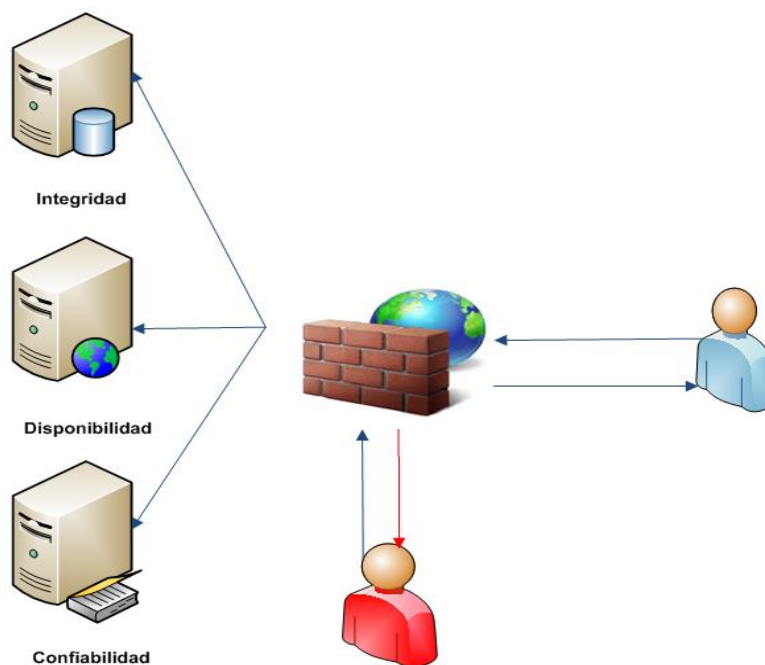


Figura 1. Ilustración objetivos en la seguridad informática

Elaborado por: Diego Poveda & Alexis Balarezo

1.4.3 Medidas de la seguridad informática

Al hablar de medidas de seguridad generalmente se menciona solamente las que tienen que ver con el nivel técnico, como pueden ser los antivirus, firewall y los sistemas que tienen que ver con las copias de seguridad.

Pero las medidas más importantes son las que tienen relación con la gestión a medio y largo plazo.

- **Medidas de gestión**

Se consideran a las medidas de gestión como una parte integral de las estrategias de una organización en la seguridad informática. Se deben realizar una vez que se tenga determinada la importancia del sistema en los objetivos de la entidad y se localice los riesgos del sistema. Al perder la integridad de la información, se deben considerar las medidas de gestión.

En el transcurso que se van desarrollando tácticas de seguridad, se generan y desarrollan herramientas importantes, las cuales, al momento de implementar medidas de seguridad son necesarias: políticas de seguridad y un plan de contingencia.

- **Medidas técnicas**

En la actualidad el número de herramientas de protección es muy extenso, todas están aplicadas a preservar la información en toda su extensión, tanto en el aspecto de la integridad, disponibilidad y confidencialidad que es lo fundamental al momento de tratar y procesar la información, es recomendable que toda organización dedique un espacio y tiempo en los objetivos para la selección y estudio de herramientas y medidas de seguridad.

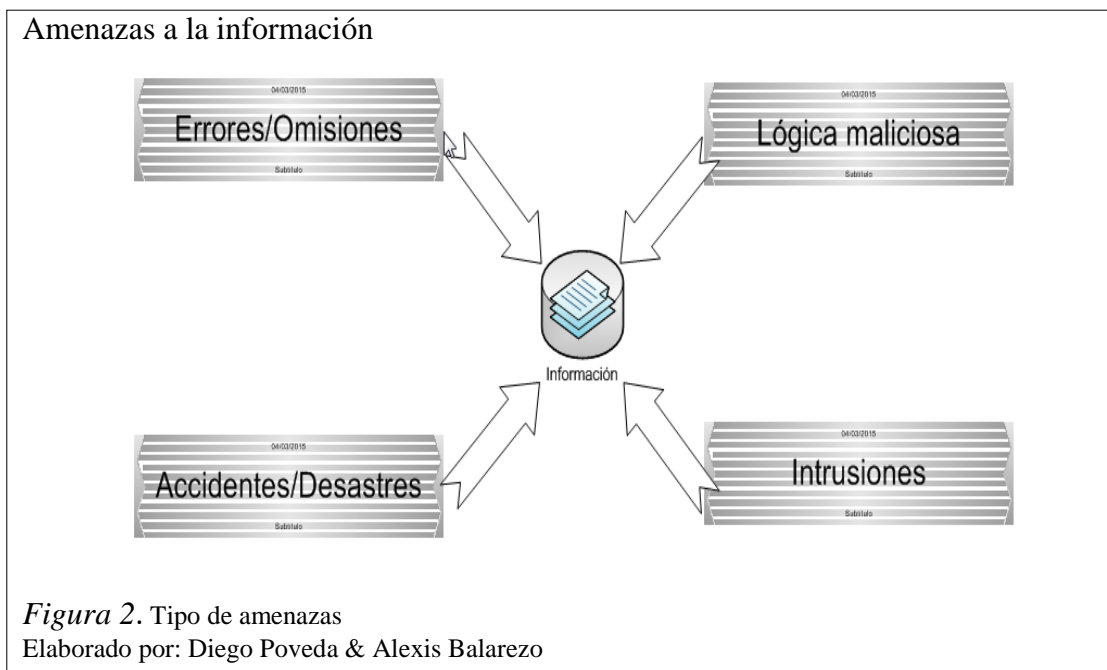
Existe una gran cantidad de técnicas consideradas como un estándar al momento de utilizarlas, un ejemplo la criptología como parte de las medidas más eficientes y utilizadas. Se considera que cualquier forma en la que se tenga redundancia en la información es considerada como una garantía a la disponibilidad frente a los eventos producidos por una amenaza.

Otra técnica de protección muy eficaz es la utilización de antivirus que están orientados a eliminar las infecciones de los sistemas, teniendo en cuenta que esto es lo esencial al momento de impedir que se produzca una lógica maliciosa, por otro lado, al proteger un sistema es necesario cualquier tipo de firewall.

1.4.4 Amenazas a la información

La información es vulnerable a una serie de amenazas, las cuales pueden producir una gran cantidad de pérdidas que de una u otra manera afecta significativamente a una entidad.

En muchos casos las amenazas pueden producir simples errores en las aplicaciones de gestión que generan un fallo en la integridad de los datos y por medio de estos errores menos significativos se puede llegar a tener un fallo principal en el sistema afectando la disponibilidad.



A medida que se desarrollan métodos en el manejo de la información personal, se han creado normas y reglas para la manipulación de estos datos dependiendo de cada país.

1.4.5 Amenazas a la seguridad de la información

Las amenazas se clasifican en cuatro grandes grupos dependiendo del nivel y propósito de afectación: interrupción, interceptación, modificación y fabricación.

Tabla 2. Amenazas según el propósito de afectación

Propósito	Descripción
Interrupción	Produce que un objeto se pierda y que sea inutilizable.
Intercepción	Interceptar información la cual está siendo transmitida.
Modificación	Acceso no autorizado el cual permite modificar un objeto del sistema.
Fabricación	Objeto que sea difícil de distinguir entre el original.

Nota. Amenazas a la seguridad de la información según el propósito
Elaborado por: Diego Poveda & Alexis Balarezo

1.4.6 Elementos considerados amenazas

En la actualidad, existe una gran cantidad de elementos que son considerados un peligro y amenazan a la seguridad de la información a continuación se detallan los principales:

- **Personas**

La mayoría de ataques son producidos por personas que intencionalmente o involuntariamente causan grandes pérdidas y producen fallos en el sistema. Se pueden dividir en dos grupos a esta clase de amenazas como atacantes activos y pasivos.

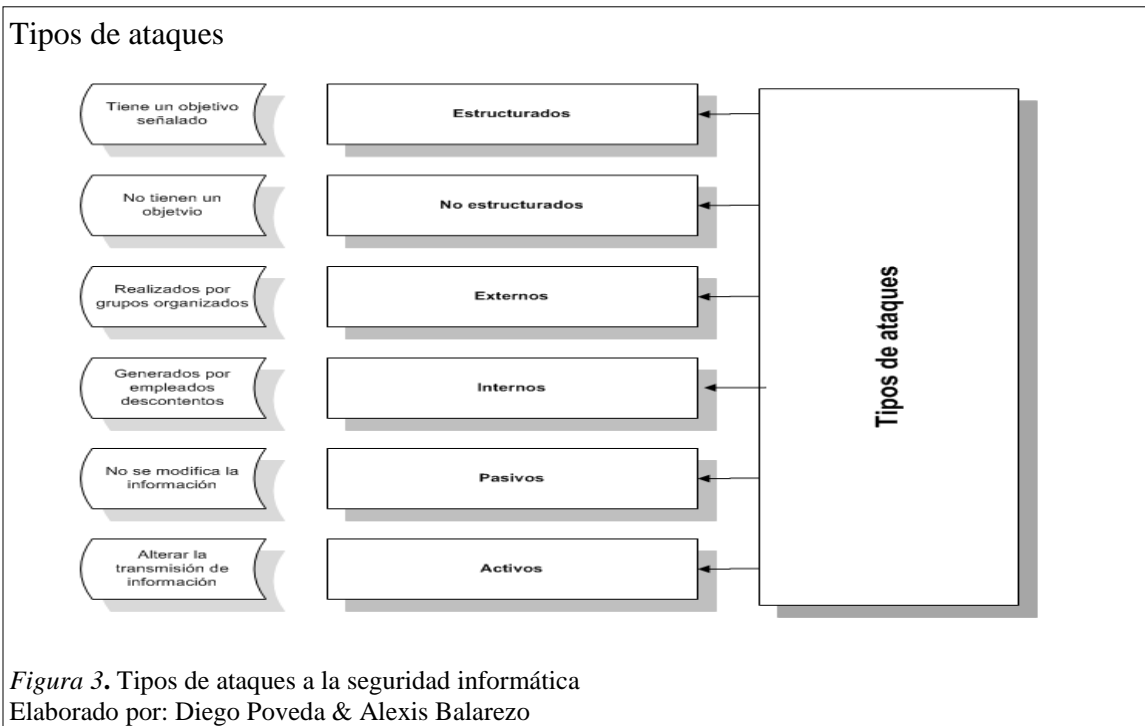
Los pasivos son aquellos que por curiosidad o investigación, ingresan a los sistemas pero no los modifican, al contrario de los activos, que son atacantes que buscan dañar el objeto alcanzado.

- **Amenazas Lógicas**

Se considera a todo software que pueda dañar lógicamente al sistema y se lo conoce como malware.

- **Software incorrecto**

Las amenazas más frecuentes y conocidas son las generadas por fallas involuntarias de los programadores al desarrollar el sistema, se produce por alguna línea de código que se encuentre incompleta que al realizar alguna determinada tarea produzca algún tipo de bucle.



1.4.7 Estándares de autenticación de usuarios PCI e ISO

- **Estándar PCI**

Los fraudes en el mundo comenzaron hace muchos años dando inicio del robo de identidad, datos personales o las tarjetas de crédito.

Con el avance de la tecnología aumenta la facilidad que se otorga al usuario en la automatización de los procesos en el envío de información personal o financiera que ofrecen las entidades, estas facilidades aumenta en paralelo con la delincuencia, en la actualidad denominados “ciber-delincuentes”, quienes de una u otra forma buscan captar víctimas de manera masiva sin exponerse físicamente.

Existen varias formas de ataques realizadas por los ciber-delincuentes, como el envío de correos electrónicos masivos, un ataque muy conocido es el phishing. El primer tipo de ataque fue dirigido a personas naturales, en el cual se procedía a enviar correos electrónicos en los que se ofrecía dinero a favor de la víctima a cambio de ayudar a liberar una supuesta cuenta bancaria congelada por alguna razón, para lo cual pedían información confidencial bancaria como requisito y un monto a la cuenta del delincuente para poder descongelar la cuenta y así devolver con las ganancias a la víctima. Esta forma es la famosa “Lotería de Bill Gates”, ofrecen una gran cantidad de dinero con la condición de que la víctima debe entregar una pequeña parte de su capital monetario.

El Estándar PCI de seguridad (Payment Card Industry Data Security Standard (PCI DSS)), fue desarrollada para la protección de datos confidenciales de usuarios titulares en las tarjetas de crédito de manera coherente y sincronizada, no es suficiente proteger solo la entidad que presta el servicio de las tarjetas de crédito sino también a las demás empresas donde serán utilizadas las tarjetas deberán proteger los dispositivos que usan estas entidades, es decir toda entidad que posee datos confidenciales del cliente de una tarjeta debe ser protegida.

Como consta en el documento Requirements and Security Assessment Procedures versión 3.0 elaborado en el 2013 se deben tomar en cuenta los siguientes puntos para cumplir con el estándar PCI DSS en referencia a la autenticación de usuarios.

- **Información aplicable a PCI DSS**

Los datos deben ser protegidos de la manera más amplia posible, es decir, la seguridad debe expandirse sin limitación alguna, para evitar la fuga de información, por este motivo se debe analizar cada uno de los elementos que participan en el procesamiento de los datos personales y confidenciales del usuario. Las normas son aplicadas en los entornos donde los datos son procesados, almacenados o transmitidos, ya sean estos manejados interna o externamente.

- **Alcance de los requisitos de PCI DSS**

Los requisitos de seguridad PCI DSS se aplican a todos los componentes del sistema, estén estos o no incluidos en el entorno. El entorno de datos del titular (CDE: cardholder data environment) lo comprenden las personas, procesos y tecnologías que almacenan, procesan o transmiten los datos del usuario de la tarjeta sea cual sea esta la información.

Se puede mencionar algunos elementos que componen el entorno donde se manejan los datos como por ejemplo: servidores de autenticación, firewalls, equipos virtuales, aplicaciones virtuales con sus respectivos hipervisores, equipos de red tanto alámbricos como inalámbricos, todos los tipos de servidores que se maneje sean de Proxy, correo, DNS, etc., aplicaciones pagadas o libres de manejo interno o externo de la información.

Para verificar que un entorno esté dentro del estándar PCI DSS se realiza una evaluación de los componentes del mismo antes mencionados, ya que la institución que busca adoptar este estándar debe informar con un alta precisión sobre los lugares y los flujos por donde es procesada y transportada la información de los usuarios, asegurando que las normas cubran cada uno de estos elementos. (Security Standards Council, 2013, págs. 10-12).

Para tener mayor precisión en cumplimiento de estas normas se recomienda realizar lo siguiente:

- La entidad identifica y documenta los datos de los usuarios dentro de su entorno, para verificar que no existan datos fuera del mismo.
- Una vez identificados y documentados los datos del usuario se analizan los resultados por parte de la entidad, para certificar que el alcance de PCI DSS es correcto y si es necesario tomar los correctivos respectivos.
- En caso de encontrar datos que estén fuera del alcance de PCI DSS, estos deben ser eliminados de manera segura, agregarlos al entorno definido o redefinir el entorno para que los datos sean incluidos.
- La entidad guarda la documentación resultante de la evaluación realizada, que muestra la determinación del entorno para los PCI DSS, lo cual servirá como referencia para una próxima evaluación.

- **Estándar ISO**

Uno de los aspectos más importantes de la seguridad informática son los usuarios, ya que ellos controlan el sistema, por lo tanto tienen acceso directo a la información, para lo cual es necesario establecer “reglas de juego”, sobre los movimientos permitidos desde el más mínimo como por ejemplo el manejo de claves personales y la incorrecta forma de creación y manipulación.

Existen normas que permiten mantener un sistema altamente protegido para lo cual se manejan algunos conceptos básicos a tratar como se manifiesta a continuación.

Un sistema seguro debe ser íntegro, confidencial, irrefutable y alcanzar una alta disponibilidad. Los estándares ISO son los que se adentran a profundidad el estudio de estos conceptos básicos, de los cuales se toman ciertos puntos relacionados en la autenticación de usuarios.

Para mantener la información en forma segura, existen varias normas que permiten realizar lo mencionado tomando para este caso de estudio de la norma ISO 27001, de la cual se describirán los aspectos puntuales en la autenticación de usuarios.

Esta norma muestra la importancia en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) y su manejo para una posible evolución. Esta norma

ISO define varios aspectos que se deben implementar para mantener el sistema protegido garantizando la integridad de la información, uno de los cuales es la gestión de acceso de usuario.

- **Control de acceso a sistemas y aplicaciones.**

El administrador de seguridad de la red, debe establecer controles para garantizar la integridad de los servicios y los datos que maneja la entidad, considerando como ataque e incidencia de seguridad grave a cualquier actividad no autorizada.

- **Identificación y autenticación de usuarios.**

La identificación y autenticación de usuario es un punto importante en la seguridad de un sistema por lo cual es necesario que cada uno de los usuarios que tengan acceso a este posean un identificador, el cual deberá ser único, sin importar el nivel o cargo que desempeñen. Este identificador será de uso exclusivo del usuario pero podrá ser usado para dar seguimiento a cada una de las actividades del individuo realizadas dentro del sistema.

- **Uso de herramientas de administración de sistemas.**

Los usuarios que tengan acceso al sistema no podrán tener acceso a los módulos de configuración de los equipos, el acceso a la configuración de los mismos la tendrá únicamente el usuario administrador, que tendrán acceso exclusivo a las aplicaciones o equipos asignados a su responsabilidad. Por este motivo es necesario reportar cada movimiento hecho dentro de los archivos del sistema.

- **Monitoreo del acceso y uso del sistema.**

El monitoreo de un sistema computarizado es necesario para la detección de anomalías, tanto de seguridad como en el funcionamiento, ayuda a dar solución en un tiempo menor al que se emplearía en caso de no contar con el monitoreo, llegando al punto de conocer cada movimiento y actividad realizada en el sistema. A continuación en la Tabla 3 se detallan tres artículos los cuales se asocian a esta normativa.

Tabla 3. *Artículos referentes al monitoreo del acceso y el uso del sistema*

Número Art.	Descripción
Art 1.	Se registra y archiva toda actividad, del sistema y la red en archivos de log o bitácoras.
Art 2.	Archivos de log, almacenarán nombres de usuarios, nivel de privilegios, IP de terminal, fecha y hora de acceso, actividad desarrollada, intentos de conexiones fallidas o acertadas, archivos a los que se tuvo acceso, entre otros.
Art 3.	Copia automática de los archivos de log y enviara hacia otra terminal.

Nota. Artículos del manual de normas y políticas de seguridad informática ISO 27000. Fuente: (Departamento de Postgrados de la Universidad del Valle de México, 2009, págs. 45-47)
Elaborado por: Diego Poveda & Alexis Balarezo

La norma ISO 27001 y cada uno de los autores de los sistemas informático buscan el resguardo y el buen uso de la información en forma preventiva y segura, para evitar el acceso a cualquier tipo de intruso mal intencionado que pueda comprometer la integridad de la empresa y con esto prevenir grandes pérdidas. (Departamento de Postgrados de la Universidad del Valle de México, 2009, págs. 40-47).

1.4.8 Arreglo RAID

Los arreglos de disco RAID se caracterizan por tener una capacidad de almacenamiento considerablemente amplia, acceso interrumpido a la información, en la actualidad, se han desarrollado dos tipos de RAID, los que son realizados por software y los que se utilizan por hardware.

- **Tipos de RAID**

Existe dos tipos de RAID los cuales permiten realizar las mismas funciones, simplemente que la arquitectura con la que se forman es diferente.

Tabla 4. *Arquitectura de los sistemas RAID*

RAID	Descripción
Software	Realiza la unión de los discos y forma los niveles de RAID, es la solución más económica ya que los dispositivos controladores de RAID tienen un alto costo.
Hardware	Tarjetas controladoras que permiten mostrar los discos al sistema

	operativo como si fuera uno solo dispositivo.
--	---

Nota. Componentes de la arquitectura RAID
Elaborado por: Diego Poveda & Alexis Balarezo

- **Niveles de RAID**

En la actualidad, existe doce tipos de RAID, pero a nivel empresarial y de servicio a usuarios home este número se reduce a seis, para determinar qué nivel es el óptimo a utilizar, se debe considerar la cantidad y la importancia de los datos que se almacenaran.

Tabla 5. *Niveles de RAID utilizados a nivel empresarial, home*

Nivel	Descripción
RAID 0	No proporciona redundancia, incrementa la capacidad de almacenamiento.
RAID 1	Nivel costoso, ya que la forma de manejar los discos es en forma de espejo.
RAID 2	En este nivel de RAID los discos carecen de la detección de errores internos.
RAID 3	Distribuye la información a nivel de bytes, redundancia por disco de paridad.
RAID 4	Distribuye a nivel de bloques la información, esta es la diferencia con el nivel 3.
RAID 5	Se crean datos de paridad para ser distribuidos a través de todos los discos.

Nota. Descripción de cada nivel RAID
Elaborado por: Diego Poveda & Alexis Balarezo

1.4.9 Cloud Computing

Se define Cloud como la tecnología que externaliza el acceso a las soluciones de software de gestión de empresas a través del internet, el cual dependiendo el servicio contratado con proveedor tendrá un bajo su costo.

Cloud Computing ofrece una infinidad de servicios, a los cuales se puede acceder por medio del internet, entre estos servicios tenemos aplicaciones informáticas, servicios de almacenamiento, correo electrónico, copias de seguridad, etc., con esto se tiene una reducción de costos, ya que el software y el hardware son totalmente independientes. El proveedor de servicio debe comprometerse con el contratante del servicio a que sus datos, programas y demás recursos sean totalmente confidenciales, fiables y estén disponibles a cualquier hora y en cualquier lugar que la empresa necesite.

Cloud Computing es un modelo de negocio y tecnología, el cual, está creciendo actualmente debido a sus grandes ventajas, las cuales, se detallaran más adelante. Los clientes de la nube pueden beneficiarse de varias maneras, tendrán un acceso continuo sin interrupciones, gran almacenamiento, alta velocidad de procesamiento dependiendo del proveedor.

Existen tres tipos de Cloud, públicos, privados e híbridos los cuales han sido clasificados basándose en la disponibilidad de los servidores.

Tabla 6. *Tipos de Cloud Computing*

Cloud	Características
Pública	Entrega del servicio a cualquiera que lo contrate, es usada por empresas que buscan poner al mercado un servicio de forma rápida.
Privada	Uso exclusivo de una empresa la cual puede gestionar la nube de forma interna o contratar los servicios de un proveedor ventaja la disponibilidad y tolerancia a fallos, inversión significativa.
Híbrida	Usada por empresas de comercio electrónico, afluencia de usuarios es variable, tienen preferencia la ejecución de las aplicaciones de la nube privada.

Nota. Características de los tipos de Cloud Computing
Elaborado por: Diego Poveda & Alexis Balarezo

- **Arquitectura de la Cloud**

La Cloud está constituida por varios elementos que permiten dar servicios a los usuarios finales según se requiera. Los servicios que puede ofrecer la nube se distribuyen de manera diferente pero todo tienen una arquitectura base, mediante la cual, el cliente accede al servicio, los elementos que constituyen a la nube son los siguientes:

- Servidores
- Sistema Operativo de Servidores
- Software de plataforma
- Aplicaciones
- Almacenamiento

Cada uno de estos elementos sirve para entregar el servicio de Cloud a los clientes, siendo los principales los servidores y el Sistema Operativo con el cual funciona el

servidor y se montarán cada uno de los servicios a prestar, tales como software de plataforma, aplicaciones y almacenamiento.

Arquitectura y servicios Cloud Computing

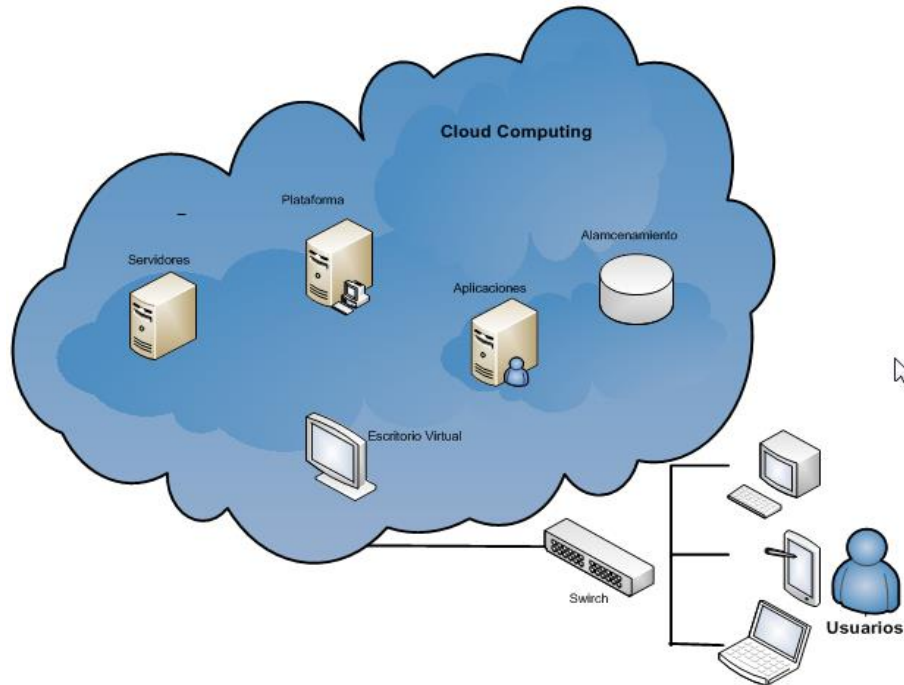


Figura 4. Arquitectura Cloud Computing
Elaborado por: Diego Poveda & Alexis Balarezo

Los servidores serán conectados directamente al internet de donde cada uno de los clientes accederá al servicio contratado. Cloud Computing funciona basada en tres puntos fundamentales, los cuales son: software, plataforma e infraestructura, que pueden trabajar en conjunto o independientemente según se requiera.

Tabla 7. Servicios fundamentales de Cloud Computing

Servicio	Descripción
Software	SaaS, aplicación completa ofrecida como servicio multitendencia denominado software bajo demanda.
Plataforma	PaaS, equipos en forma virtual e instalados para que el usuario haga uso del servicio acorde a las necesidades.
Infraestructura	IaaS, almacenamiento básico y las capacidades de cómputo como servicios estandarizados en la red.

Nota. Descripción de servicios fundamentales de la Cloud Computing
Elaborado por: Diego Poveda & Alexis Balarezo

- **Características**

Los servicios de la Cloud Computing están regidos a métricas de consumo en lo cual se basa el proveedor para establecer el monto de cobro

Tabla 8. *Características principales Cloud Computing*

Características	Principios
Auto reparable	En caso de fallo el último backup pasa a funcionar de forma primaria.
Estabilidad	Se garantizan la recuperación del sistema de forma inmediata.
Escalable	Puede aumentar su capacidad de carga con el aumento en la infraestructura.
Virtualización	Las aplicaciones pasan a ser independientes del hardware en el que se ejecutan.
Multipropósito	Servicios a varios clientes a la vez compartiendo infraestructura.
Agilidad	El usuario manipula sus aplicaciones de acuerdo a las necesidades.
Accesibilidad	Acceso desde cualquier dispositivo que cuente con una conexión a internet
Seguridad	Se maneja controles de seguridad para que la información no pueda ser extraída.

Nota. Descripción de características de la Cloud Computing

Elaborado por: Diego Poveda & Alexis Balarezo

- **Ventajas y desventajas**

Entre las principales ventajas que se pueden tomar en cuenta en la Cloud Computing, las cuales, permiten la elección de este tipo de sistema para ser implementado en una empresa están las siguientes:

Tabla 6. *Descripción de las ventajas y desventajas de la Cloud Computing*

Ventajas	Acceso a la información desde cualquier lugar del mundo mediante internet.
	Ejecución de servicios mucho más rápido que en una infraestructura física.
	Disposición a nuevas funcionalidades dependiendo la disponibilidad.
	Actualizaciones automáticas de las aplicaciones sin riesgo.
Desventajas	El cliente pasa a depender del proveedor del servicio.
	El internet es un factor principal para el cliente.
	La información deberá pasar por varios nodos para llegar a su destino
	El incremento de clientes podría llegar a la saturar los servicios de a Cloud.

Nota. Ventajas y desventajas encontradas en la Cloud Computing

Elaborado por: Diego Poveda & Alexis Balarezo

- **Redes empresariales en la Cloud Computing**

El movimiento tecnológico ha evolucionado en el campo empresarial, por lo cual muchas de las empresas han optado por el cambio de infraestructura física a una estructura virtual contratada en la Cloud, aunque muchas de las veces las empresas han dudado de hacerlo por ciertos tabús tecnológicos, creados en el medio, sobre todo en cuanto a la seguridad y privacidad de sus datos se refiere, esto se presenta por el desconocimiento de las funcionalidades y el servicio que ofrece.

Según el reporte de investigación realizado por Verizon Data en el año 2013 el 86% de las brechas de seguridad se debieron al uso de contraseñas y usuarios robados. En el 2015 el 60% del presupuesto de los jefes de informática para la seguridad de los sistemas oscilarán entre un 30% y un 40% como financiamiento de evaluaciones de amenazas a las empresas. Esto implica que la demanda aumentará en cuanto a las implementaciones de nubes privadas. Un ejemplo local de este tipo de proveedor es la empresa EJE Comunicaciones, que ofrece el servicio de respaldo de información en la nube y adicional ofrece varios tipos de servidores virtuales con diferentes sistemas operativos, para que las empresas puedan desarrollar sus procesos internos.

1.4.10 OSSIM.

En la actualidad OSSIM se identifica por ser una herramienta que ayuda a solventar y responder los ataques que pueden pasar desapercibidos por los IDS convencionales, permitiendo administrar los diferentes logs que se obtiene de la red de una manera sencilla para así lograr importantes informes. (Miller, Harrys, Harper, & VanDyke, 2010, págs. 205-207).

OSSIM está formado por dos gestores de eventos SEM y SIM.

Tabla 7. *Partes que constituyen a OSSIM*

Tipo Gestor	Descripción
SEM	Monitoreo en tiempo real, control dinámico de la consola para poder visualizar y administrar los eventos.
SIM	Permite un análisis más histórico, información flexible.

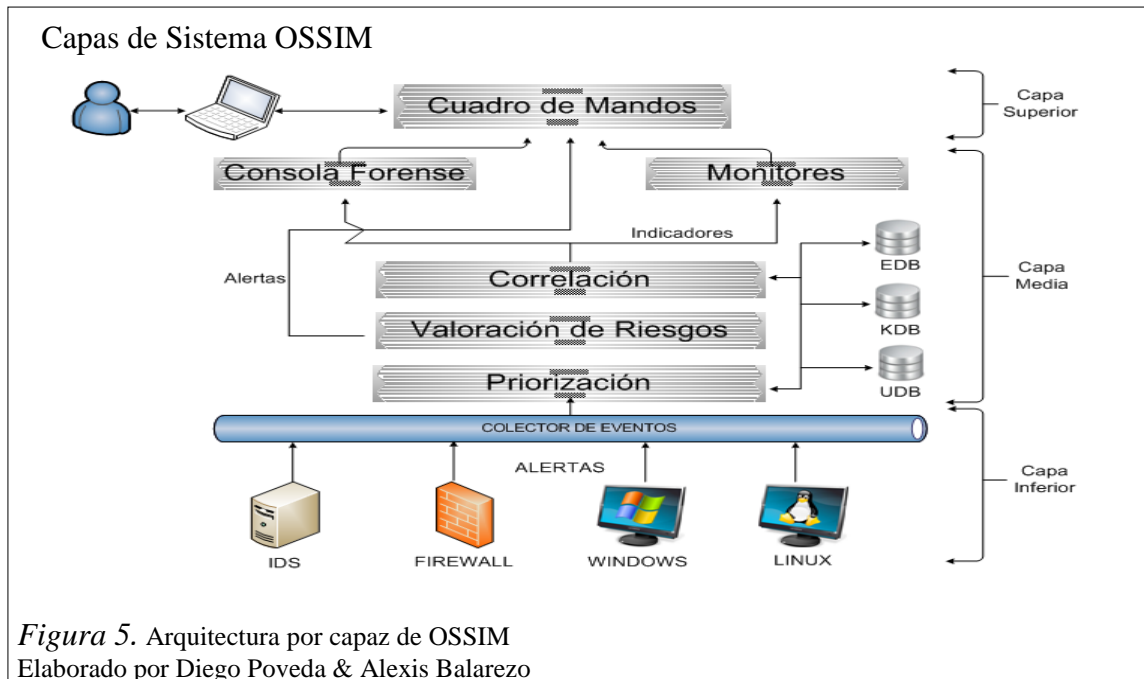
Nota. Descripción de los componentes de OSSIM
Elaborado por: Diego Poveda & Alexis Balarezo

Una de las ventajas de OSSIM, es el almacenamiento de la información que se obtiene de los eventos o logs a largo plazo, ya que con esta información se puede descubrir una violación en la seguridad, estos datos son muy utilizados en la informática forense ya que no es muy probable identificar una amenaza en tiempo real siempre es necesario analizarla información almacenada para localizar algún patrón que identifique a un ataque. (Estación Informática, 2013).

- **Arquitectura.**

El sistema OSSIM al considerarse un administrador de herramientas de monitorización cuenta con una arquitectura funcional la cual se divide en tres capas para dar el tratamiento adecuado y seguro a los datos que se recolecta en su funcionamiento, cada una de estas capas cumple con tareas definidas cuya descripción se presenta a continuación:

- **Preprocesado (capa inferior):** Capa más baja del OSSIM, donde se colectan y correlacionan los eventos, los cuales, son enviados por los sensores o monitores hacia el sistema núcleo.
- **Postprocesado (capa media):** Interpreta cada evento enviado por cada agente o sensor y lo traduce para que el administrador lo interprete de mejor manera, esto es manejado por el motor de correlación, es decir que relaciona los datos que ingresan y ofrece un dato de salida legible generando los distintos tipos de avisos o alertas dependiendo el caso.
- **Front-end (capa superior):** Permite interactuar con la herramienta tanto en la visualización de eventos como en la configuración de las herramientas. Front-end pasa a ser la capa de administración del sistema la que se puede acoplar a las necesidades de la entidad en la que va a funcionar.



- **Herramientas integradas en OSSIM**

Existe una gran cantidad de herramientas de monitoreo y detección integradas en la funcionalidad de OSSIM, para la presente investigación se analizarán las siguientes herramientas que son consideradas las más importantes.

- **OSSEC.**

Es un sistema de monitoreo y detección de intrusos, en otras palabras constituye un IDS basado en host, que gestiona la información generada de los eventos para la obtención y verificación de la información, esta herramienta se constituye en un modelo cliente-servidor, logrando que se administre un servidor centralizado el cual recibirá y gestionará la información recolectada por los agentes que son los equipos monitoreados. Gracias a su alta compatibilidad OSSEC puede funcionar en varios sistemas operativos como Windows, Linux, en incluso existe soporte para Solaris, las características más relevantes de estas herramientas son:

- Comprobación de la integridad de los sistemas.
- Verificación y supervisión de los registros de los sistemas operativos Windows.

- Envío de la información obtenido de los sucesos en tiempo real para una respuesta activa.

OSSEC permite instalarlo en dos formas dependiendo la necesidad en modo local o en modo cliente-servidor.

Tabla 8. *Formas de instalación de la herramienta OSSEC*

Modo Instalación	Descripción
Local	En este modo se tiene al cliente y al servidor como un solo host,
Cliente-Servidor	Toda la información que se obtenga de la detección de anomalías es enviada a un servidor centralizado.

Nota. Descripción de las formas de instalación de la herramienta OSSEC

Elaborado por: Diego Poveda & Alexis Balarezo

- **NMAP.**

Es un escáner de red, que permite crear inventarios de los sistemas o host activos en la red, en otras palabras es una herramienta para la exploración de redes, permite escanear los puertos de las máquinas que se encuentra en la red, se puede identificar si un puerto está abierto, cerrado o se encuentra protegido, determina que servicios se encuentran utilizados por los equipos de la organización, incluso muestra la información del sistema operativo.

La información primordial que muestra NMAP es la tabla de puertos. La tabla muestra el número de puerto y protocolo, el nombre del servicio y su estado, los estados puede ser: open, filtered, closed, unfiltered (no filtrado).

Tabla 9. *Estado de puertos en la lista de información de NMAP*

Estado	Descripción
Abierto	Esperando conexiones o paquetes en el puerto.
Filtrado	Cortafuegos o filtro, se encuentra bloqueando el acceso al puerto.
Cerrado	Ninguna aplicación escuchando, aunque podrían abrirse en cualquier instante.
No Filtrado	Nmap no puede determinar si se encuentran abiertos o cerrados.

Nota. Descripción del estado de puertos de la herramienta NMAP

Elaborado por: Diego Poveda & Alexis Balarezo

NMAP muestra e informa las combinaciones de estados como: open|filtered y closed|filtered cuando no puede determinar en cuál de los dos estados está asignado al puerto. NMAP ofrece información de los protocolos IP soportados, en vez de puertos abiertos.

- **NAGIOS.**

Esta herramienta posiblemente es el software de código abierto para el monitoreo y la gestión de red más utilizado en la actualidad, permite verificar en forma activa la disponibilidad de los servicios y dispositivos de la red, todos los sucesos que se generen en la disponibilidad se muestran como alertas, todo esto puede ser configurado dependiendo la necesidad del administrador, a continuación los principales servicios que son monitoreo por NAGIOS:

- POP3
- HTTP
- SMTP
- ICMP
- SNMP

Adicional a los servicios que se tiene por defecto en la herramienta se tiene la posibilidad de configurar nuevos plugins y con esto poder monitorear el uso de los discos, la memoria de los dispositivos e incluso el estado de los puertos, se tienen la posibilidad de configurar el envío de información mediante las alertas a los diferentes administradores de la red, dependiendo la gravedad de la situación. (Dorat & Moran, 2015, págs. 24-26).

NAGIOS tiene la función de distinguir entre un host inaccesible a uno que se encuentra sin servicio, esto se logra configurando la jerarquía de red, se puede configurar manejadores de sucesos o eventos los cuales permiten reaccionar y solventar algún tipo de inconveniente presentado con los servicios. Permite el monitoreo de equipos con redundancia, con este soporte se puede monitorear equipos remotos utilizando túneles SSL cifrados, toda la información que se obtiene se la puede visualizar en forma gráfica mediante

su interfaz web y generar informes los cuales contendrán información gráfica del comportamiento de los sistemas que se encuentran en monitoreo. (Párrigas, 2015, págs. 13-18).

Tabla 10. Descripción y funcionalidades de elementos de arquitectura de OSSIM

FUNCIONALIDADES DE COMPONENTES DE ARQUITECTURA OSSIM			
CAPA	COMPONENTE	FUNCIONES	DESCRIPCIÓN
Superior	Cuadro de Mandos	Presentación visual de eventos y alertas	Permite la visualización de eventos y alertas generadas en la red con formato legible y comprensible para el administrador
Media	Consola Forense	Acceso a información	Accede a toda la información recogida y almacenada por el colector de eventos de manera centralizada
	Monitores	Monitorear procesos	Encargados de monitorear los procesos que se presentan en la red en sus diferentes casos
	Correlación	Procesamiento de datos	Procesa datos de entrada enviada por los sensores y entrega datos de salida
	Valoración de Riesgos	Clasificar niveles de riesgo	Valora la importancia cada evento suscitado en la red basándose en factores como el valor del activo, tipo de amenaza y probabilidad de que esta suceda
	Priorización	Evaluar importancia de eventos	Evalúa los eventos según su nivel de importancia para que este sea atendido teniendo niveles bajo, medio y alto
	BDD	Almacenar información	Almacena todo tipo de datos de la red. Dependiendo el tipo de datos tenemos tres BDD: EDB almacena todos los eventos generados en la red. KDB es la BDD de framework en donde se guardarán todos los parámetros de nuestra red. UDB almacena los datos de uso realizado por el usuario.
Inferior	Colector de Eventos	Recolección de eventos	Recolecta todos los eventos generados en la red para posteriormente ser procesados
	Generadores de Eventos	Dar servicio a usuarios	Todo equipo conectado a la red generará eventos con cada acción realizada dentro del mismo

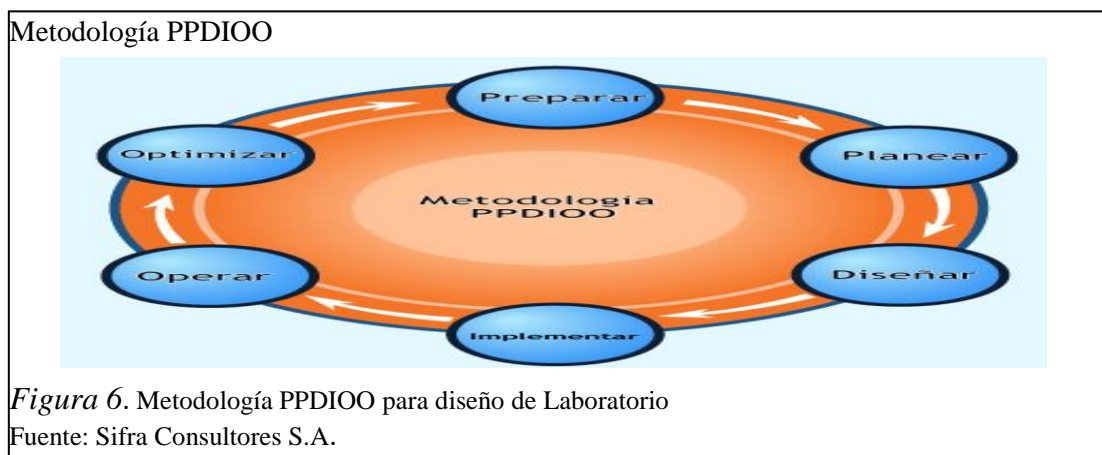
Nota. Descripción de funcionamiento de los elementos de la arquitectura de OSSIM

Elaborado por Diego Poveda & Alexis Balarezo

CAPÍTULO 2

DISEÑO E IMPLEMENTACIÓN

El siguiente diseño e implementación se realizó basado en la metodología PPDIO que es exclusiva para el ciclo de vida de una red. Esta metodología permite que una organización maneje y mejore de manera continua su red, sin que se presente interrupción en la operación y adaptándose a las necesidades presentadas y de forma dinámica, la optimización depende directamente a una buena supervisión en la fase de operación.



2.1 Fase de preparación

Los altos costos que representan el diseño y construcción de una red física están generando que los administradores de red opten por contratar recursos virtuales los cuales pueden ser escalables dependiendo los requerimientos del cliente.

En la presente fase se identificará y se visualizará las partes más destacadas que conformarán la arquitectura del laboratorio, para la preparación del diseño se analizará y aprovechará la variedad de ventajas que brinda las tecnologías de la información.

Antes del diseño del laboratorio de la siguiente investigación se debe considerar que una red es un conjunto de dispositivos físicos “hardware” y de programas “software”, mediante la cual se pueden comunicar computadores para compartir recursos y distribuir el trabajo. A cada equipo conectado a la red se los denomina “nodo”.

Tabla 11. *Elementos de una red*

ELEMENTOS NECESARIOS DE LA RED
a. Los programas serán aquellos que gestionan la comunicación entre los nodos y los periféricos.
b. La tarjeta de comunicación instalada en cada una de las computadoras conectadas o nodos.
c. El cableado o medio que los une.

Nota. Descripción de los elementos de una red
Elaborado por: Diego Poveda & Alexis Balarezo

Las redes difieren entre sí por los servicios que prestan a los usuarios o por la comunidad de usuarios atraídos por el servicio.

Una vez que se tiene claro los elementos que componen a una red, se debe verificar la estructura y los recursos necesarios para el funcionamiento de la misma.

Tabla 12. *Estructura de una red*

ESTRUCTURA DE UNA RED
a. Almacenamiento
b. Plataforma
c. Servicios
d. Seguridad

Nota. Descripción de la estructura de una red
Elaborado por: Diego Poveda & Alexis Balarezo

Almacenamiento

Tomando en cuenta cada una de las características de las tecnologías a usar y para el cumplimiento de los requerimientos de la investigación se procederá con el uso de un servidor RAID 5 el que garantizará la disponibilidad de la información, en el cual se almacenara toda la información de la red.

Plataforma y servicios

Para el diseño del laboratorio de pruebas es necesaria una Cloud Computing de tipo privada ya que su uso es exclusivo de una empresa y se puede gestionar la nube de forma interna. Para los requerimientos de la siguiente investigación se configurara un servidor Cloud Computing tipo PaaS debido a que su virtualización emula el

funcionamiento de equipos reales que generan eventos los cuales serán configurado como un servicio, permitiendo el montaje de un laboratorio de pruebas apto para el uso y manipulación del sistema de monitoreo OSSIM el cual permitirá administrar la información de las herramientas de seguridad en la red.

Seguridad

Es necesario el uso de un sistema OSSIM de código abierto ya que el objetivo de la investigación es mejorar su funcionamiento mediante la innovación de su código por lo cual se procede al uso de AlienVault OSSIM.

2.2 Fase de planificación

Para el presente diseño es necesario el cumplimiento de los siguientes requerimientos descritos a continuación en la Tabla 13:

Tabla 13. *Requerimientos para el diseño del Laboratorio*

No.	Requerimiento
Almacenamiento	
1	Sistema Operativo libre diseñado para almacenamiento remoto en una red utilizando NAS, para la aplicación de protocolo NFS
2	Sistema adaptable a cualquier ordenador con el objetivo de reducir costos y aumentar la flexibilidad
3	El sistema debe permitir gestionar los volúmenes de datos y su uso compartido
4	El sistema permitirá la configuración de un arreglo de discos duros para protección de la información
5	La información deberá ser distribuida en el conjunto de discos para obtener redundancia al presentarse un fallo
Plataforma y Servicios	
6	Es necesario una infraestructura robusta y tolerante a fallos sin tener un gasto en licenciamiento
7	Plataforma que permita aplicar diversas técnicas de control de virtualización al mismo tiempo, diferentes sistemas operativos, almacenamiento centralizado y manejo multiservidor centralizado
8	Las máquinas virtuales deben ser totalmente independientes y permitir configurar/asignar los recursos de manera flexible
9	La plataforma deberá contar con propiedades de alta disponibilidad y balanceo de carga, ya que las VM y su VDI se deberán mover de un nodo a otro sin presentar tiempos de inactividad
10	La plataforma deberá permitir una conexión NFS
Seguridad	
11	Sistema open source que permita la gestión de la información de seguridad de una red
12	Es necesario que el sistema permita integrar soluciones de código libre para la

	monitorización y detección de patrones de redes
13	Es necesario que el sistema recolecte toda la información de los diferentes plugins para integrar e interrelacionar entre sí y obtener una visualización única del estado de la red con el mismo formato
14	Es necesario que el sistema permita crear y gestionar políticas de seguridad, definir reglas de correlación y enlazar diferentes herramientas de monitoreo y detección

Nota. Descripción de requerimientos para el diseño del laboratorio de pruebas
Elaborado por Diego Poveda & Alexis Balarezo

2.3 Fase de diseño

Para la estructuración del laboratorio se unen todos los componentes a utilizar para que tenga un funcionamiento síncrono el cual permita desempeñar cada punto de esta investigación entre los cuales están los siguientes:

- Servidor RAID.
- Servidor CLOUD
- Plataforma CLOUD COMPUTING
- Sistema OSSIM
- S.O. montables

Cada uno de los elementos deben estar instalados de manera estable como menciona el capítulo 2 de la investigación tomando en cuenta cada uno de los requerimientos, los mismos quedarán estructurados de la siguiente forma como muestra la Figura 8.

2.3.1 Servidor RAID

Para la siguiente investigación e implementación se procederá a configurar un RAID 5 basado en software, que presenta un nivel superior de redundancia y confiabilidad en el manejo de los datos en comparación con los niveles 0, 1, 3, la implementación se la realiza utilizando las siguientes tecnologías de la información:

- FreeNAS 9.3 sistema operativos, el cual permite crear un esquema de almacenamiento en red (NAS), mediante este sistema se configura el nivel RAID 5, para tener la redundancia de información y conseguir alta disponibilidad.
- 3 Disco Duros de la misma capacidad de almacenamiento, los datos de paridad consumirán un disco, dejando los discos N-1 que será el espacio de almacenamiento útil.

Explicación matemática del funcionamiento del arreglo RAID nivel 5

2 Disco duros (almacenamiento)
1 Disco duro (paridad)

D1 = 1 TB D2 = 1 TB D3 = 1 TB

Almacenamiento = (N-1) (Dn...)
(3-1) (1 TB, 1 TB) = 2 * (1 TB) = 2 TB

XOR entre los discos.

D1 = 00000101
D2 = 00000011

DP = 00000110 D1 XOR D2

DP = D1 XOR D2

En caso de falla para recuperar la información se considera la relación siguiente:

D1 = D2 XOR DP = D1
D2 = 00000011
DP = 00000110

D1 = 00000101 D2 XOR DP

Figura 7. Cálculo matemático funcionamiento RAID 5

Elaborado por: Diego Poveda & Alexis Balarezo

2.3.2 Servidor Cloud Computing

Para la presente investigación y la implementación del laboratorio de pruebas en la nube se analizará e implementará la herramienta CITRIX XenServer que permite emular varios sistemas y su hardware en una infraestructura centralizada, no se utilizará OpenStack ya que al momento paso de ser una herramienta libre a una sistema de pago.

XenServer posee un reducido Kernel de Linux, para el control de los dispositivos virtualizados y el hardware físico, para la instalación es necesario algunos requerimientos esenciales.

- **Hardware**

- CPU, uno o varios con una arquitectura de 64 bits, procesador con múltiples núcleos mínimo de 1.5 GHz.
- Para el soporte de equipos Windows, se necesita que el CPU soporte las tecnologías de virtualización Intel-TV o AMD-V.
- RAM, mínimo de 2GB para un óptimo funcionamiento.
- Disco Duro, para no presentar problemas al momento de la instalación se recomienda mínimo disco de 60GB.

2.3.3 Sistema OSSIM

Para proceder con la implementación del OSSIM en la Cloud Computing es necesario cumplir con ciertos requerimientos básicos para una ejecución óptima.

- **Requerimientos de Software.**
 - Software de instalación del S.O
 - Perfil de instalación predefinido
 - Configuración tarjeta de red virtual
 - Conexión con servidor de almacenamiento
- **Requerimientos de hardware**
 - Memoria RAM mínima libre de 2GB en la plataforma
 - Espacio libre en el servidor de almacenamiento
 - Tarjeta de red compatible con el sistema
 - Procesador mínimo multinúcleo de 1.5 Ghz

Diagrama del laboratorio de la presente investigación

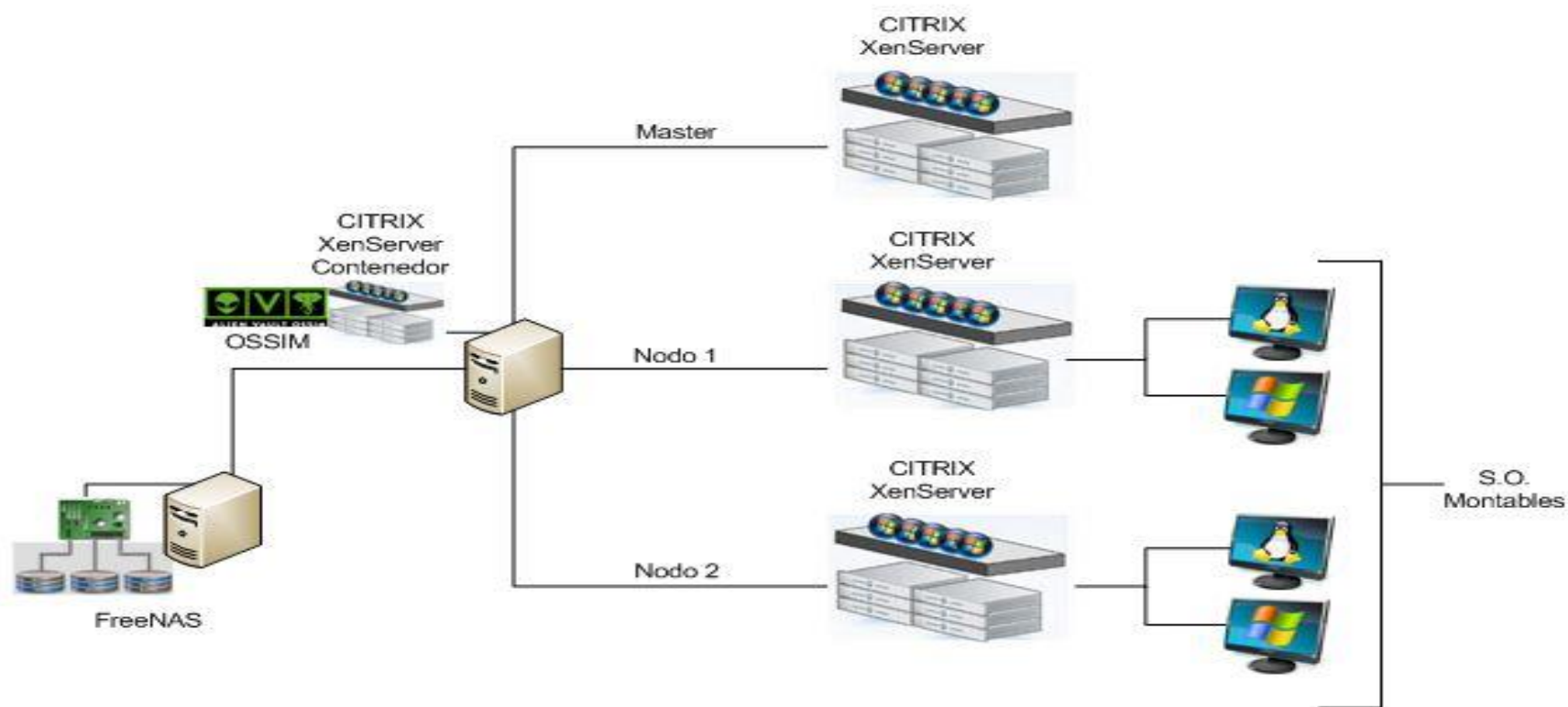


Figura 8. Diagrama del laboratorio de pruebas
Elaborado por: Diego Poveda & Alexis Balarezo

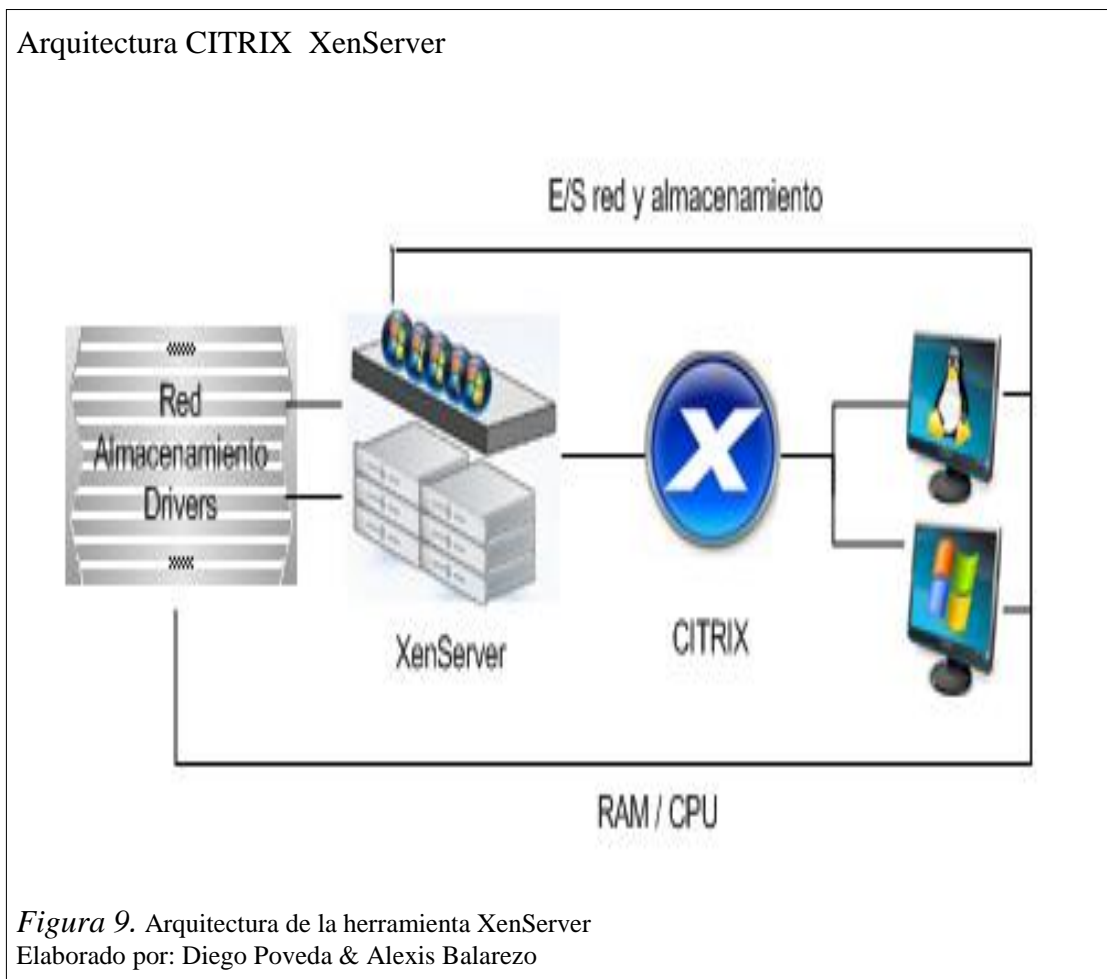
2.4 Fase de implementación

Una vez establecidos los parámetros de diseño y los requerimientos se procede con la implementación del laboratorio de pruebas.

2.4.1 Instalación Cloud Computing

Citrix XenServer está basado en Linux mediante la distribución de Centos, este sistema es capaz y está desarrollado para manejar una plataforma de virtualización de código abierto.

La plataforma de XenServer está diseñada para administrar tanto sistemas Windows como Linux a nivel de equipos home y servidores, permite ofrecer almacenamiento ilimitado, todo esto dependiendo la infraestructura del proveedor y la capacidad de escalabilidad que posea.



La arquitectura de XenServer permite el manejo de plataformas virtualizadas tanto de 32 y 64 bits gracias a la extensión para virtualización Intel-VT o AMD-V, dependiendo del procesador que se esté utilizando los cuales no son compatibles físicamente entre sí.

Se debe mencionar que el sistema XenServer no tiene un consumo de memoria RAM significativo pero al implementar los sistemas virtuales se debe considerar la memoria necesaria para cada Sistema Operativo que consumirán la infraestructura y recursos de la memoria física del servidor, por lo cual dependiendo el número de virtualizaciones a realizar se prepara el servidor.

XenServer es un sistema y se lo debe arrancar desde un recurso de almacenamiento portable con la respectiva imagen, para la presente instalación se utilizará una ISO, esta es necesaria para comenzar con la instalación como cualquier Sistema Operativo normal. Posteriormente se realizan las configuraciones según se requiera como son: idioma, medios de instalación, password de root, etc., entre los requisitos está la introducción de una dirección IP la cual se recomienda que sea configurada como estática, la cual permitirá administrar el servidor de forma remota, no es recomendable establecerla con DHCP ya que se presentara conflictos con los dispositivos de la red.

Finalizada la instalación del servidor con los parámetros solicitados por el asistente de instalación del sistema se debe comprobar la validación de los datos ingresados, esto se lo realiza mediante la navegación por las opciones que despliega el sistema como por ejemplo en Network and Management Interface donde se encuentran las configuraciones de red y hostname del sistema.

Una vez confirmado que las configuraciones son correctas, se procede a la instalación de un cliente, el cual servirá para administrar el servidor remotamente, en la actualidad el sistema administrador es XenCenter que está provisto en la imagen ISO de XenServer, con la cual se instaló el sistema del servidor. Se debe instalar la aplicación cliente sin ninguna especificación en especial, una vez que se tenga instalado se debe establecer la conexión al servidor, agregando un nuevo servidor al a consola de administración mediante la opción de añadir conexión de XenCenter, se solicita la dirección IP, usuario y contraseña, para este caso es el root.

Establecida la conexión se puede comenzar con la creación de nuevas máquinas virtuales en la nube tomando las opciones que ofrece la herramienta cliente XenCenter, que muestra las múltiples posibilidades para instalar los Sistemas Operativos que pertenecerán a los dispositivos virtuales, los cuales deberán ser instalados por medio de un CD de instalación, imagen ISO o en el caso de algunas distribuciones de Linux desde una URL.

Debido a que la herramienta no trae configurada la opción que permite instalar un sistema directamente desde una imagen ISO que se encuentra en el sistema o en algún dispositivo de almacenamiento es necesario configurar un repositorio el cual permita incluir la imágenes en el servidor para proceder con la creación de dicho repositorio, es necesario seguir los pasos e ingresar los comandos que se detallan a continuación.

- Crear una ruta donde se almacenarán las imágenes ISO en el servidor
- Ejecutar los comandos para establecer como repositorio la ruta creada:

```
mkdir /var/xen/repoISO  
xesr-create name-label=ISOs type=isodeviceconfig:location=  
/var/xen/repoISOdevice-config:legacy_mode=true contecnt-type=iso
```

Mediante esto se crea el nuevo repositorio con el nombre de ISO, una vez que se tiene accesos a repositorio creado se añade las imágenes ISO en la ruta establecida.

Para la vitalización de cada sistema se debe colocar las configuraciones requeridas para el correcto funcionamiento, como son la capacidad de disco duro, memoria RAM y las interfaces de red. En el caso de la memoria RAM se tiene un límite, debido a que el total de esta será igual al total de la memoria física que se usa el servidor, cada equipo usará parte de ella sumando la capacidad de memoria configurada de cada máquina virtual hasta llegar al límite.

2.4.2 Instalación OSSIM.

El sistema OSSIM a utilizar en la presente investigación es AlienVault, el cual se lo encuentra en su página oficial al tratarse de un software de código abierto. Este sistema de monitoreo permite su instalación con Perfil Servidor o un Perfil Sensor.

El primer perfil mostrado como opción es en modo servidor, siendo este el perfil más completo contando con las funciones de MONITOR, SENSOR e INTERFAZ GRÁFICA.

La funcionalidad monitor del sistema trabaja mediante peticiones, es decir el sistema envía mensajes a los equipos conectados y configurados en la red a monitorear y con la respuesta obtenida de estos mostrará la información solicitada, detallando eventos o anomalías suscitadas en este pedido, todo esto será guardado en los archivos de logs correspondientes.

La segunda funcionalidad es el modo sensor, como lo dice su nombre el servidor estará alerta a cualquier anomalía presentada en los equipos conectados a la red tomando en cuenta los logs generados por estos dispositivos, siendo esto posible mediante la instalación de un agente en los equipos que se encargará del envío de las notificaciones.

La interfaz gráfica tendrá la función de mostrar cada uno de los eventos suscitados en la red ya sean estos captados por un sensor o un monitor, la visualización es gráfica mediante un navegador web con el uso de la dirección IP configurada al momento de la instalación. En la interfaz encontraremos distribuidas cada una de las herramientas que contiene el sistema entre los cuales encontramos: NAGIOS, NMAP, OSSEC.

El segundo perfil que permite escoger el sistema es el modo sensor, teniendo como única funcionalidad la captura de alertas generadas por los equipos conectados a la red, en este caso se usa este perfil de instalación al tratarse de una red extensa con el objetivo de instalar un servidor núcleo y varios sensores distribuidos que se encarguen de manejar el control de cierto segmento de red.

Al tratarse de un sistema basado en la distribución de Linux Debian se la realizará con los procesos similares a la instalación de la distribución antes mencionada, teniendo en

cuenta el perfil que se vaya a utilizar de AlienVault, para el caso de la investigación se toma el perfil de servidor.

Seleccionado el perfil se deberán ingresar las configuraciones de red con las que funcionará el sistema, entre los que se encuentra la dirección IP, tomando en cuenta y teniendo gran importancia esta debe encontrarse en el rango de direcciones válidas de la red para tener conexión con los equipos a monitorear. Una vez ingresados estos datos de configuración el proceso de instalación avanzará automáticamente con el resto de configuraciones por defecto.

Una vez terminada la instalación el sistema mostrará la consola de administración del sistema en donde podremos adecuar sus características a los requerimientos.

2.5 Fase de operación

En esta fase se detallará el análisis funcional del laboratorio de pruebas implementado en base a los requerimientos.

2.5.1 Análisis funcional Cloud Computing

XenServer es un sistema basado en una plataforma de virtualización orientada a un nivel empresarial, esta plataforma permite la creación de una nube la cual ofrece características para la implementación de un Data Center en forma virtual.

Tabla 14. *Funcionalidades XenServer 6.5 (Free)*

Funcionalidades	Descripción
XenMotion	Trasladar máquinas virtuales de un nodo a otro, si perder la conexión.
StorageMotion	Mover las maquinas en ejecución y el disco virtual entre nodos, permitiendo cambiar de un entorno de desarrollo a uno de producción.
Alta Disponibilidad	Permite reiniciar los sistemas desde el Hipervisor al presentarse una fallo.
Snapshots	Permite capturar el disco virtual para realizar un backup.
Memoria	Compartir la memoria que no está en uso del servidor en las máquinas.
Conversión Manager	Convertir las maquinas VMware para que se ejecuten en XenServer.
Pools Heterogéneos	Permite soportar Full XenMotion y StorageMotion.

Administración del Rol	Permite la administración por niveles de acceso al Pool.
Reporte y Alertas	Permite tener notificaciones de rendimiento de las máquinas virtuales.
WorkloadBalancing	Crear reglas para mantener el rendimiento en la plataforma.
vGPU	Permite el soporte GPU basado en hardware.

Nota. Descripción de funcionalidades del sistema XenServer 6.5

Elaborado por: Diego Poveda & Alexis Balarezo

El la figura 10 se muestra el funcionamiento y la ejecución de la alta disponibilidad de la infraestructura de la Cloud Computing que en la presente investigación es XenServer, se puede verificar que al momento de producir un fallo de hardware en uno de los nodos, el software de alta disponibilidad que se ejecuta en la Cloud Computing es capaz de arrancar automáticamente los servicios en cualquiera de los otros nodos, cuando el nodo que ha fallado se recupera, los servicios son nuevamente migrados al nodo original. La capacidad de recuperación automáticamente de los servicios en este caso las máquinas virtuales nos garantiza la alta disponibilidad de los servicios ofrecidos por la nube, reduciendo así la percepción de fallo por parte de del cliente.

Análisis funcional CITRIX XenServer

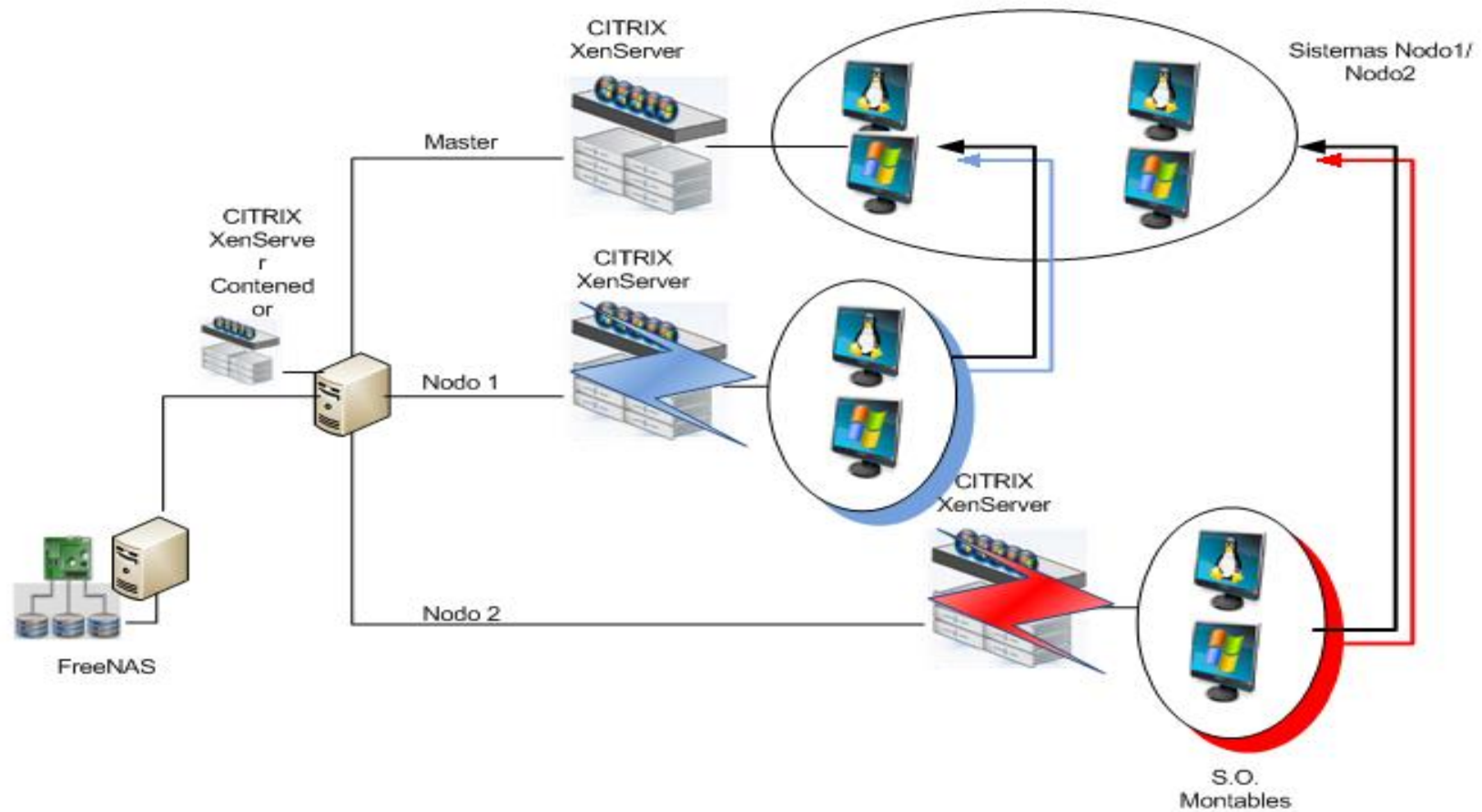


Figura 10. Funcionamiento CITRIX XenServer
Elaborado por: Diego Poveda & Alexis Balarezo

2.5.2 Análisis funcional OSSIM

OSSIM al tratarse de un sistema contenedor de varias herramientas las cuales funcionan basándose en los eventos (logs) generados dentro de la red que siguen un flujo de procesos para llegar a visualizar cada evento suscitado de manera que el administrador pueda interpretar fácilmente. El flujo de datos comienza en cualquier equipo conectado a la red, el cual, desempeña varias actividades o tareas, las mismas que al completarse generarán un evento el cual será captado por los sensores y/o agentes de OSSIM el cual maneja patrones para saber si el evento generado representa una alerta.

Al ser identificado un evento como alerta, el mismo es enviado al colector de eventos el cual los recibe a través de los diferentes protocolos abiertos de comunicación. El parser normaliza cada uno de los eventos y los almacena, en esta capa de OSSIM se clasifican las alertas según la prioridad y la política de seguridad definida, a su vez se valora el riesgo de esta de manera instantánea y en caso de ser necesario al tener un riesgo alto se enviará la alerta al cuadro de mandos.

En caso de encontrarse una alerta desconocida esta será cualificada mediante los procesos de correlación para su posterior almacenamiento, priorización y valoración de riesgo. Una vez terminado el proceso de priorización y valoración de riesgos estos eventos pasan a un monitor dependiendo el tipo de evento como por ejemplo el monitor de riesgo, monitor de uso, monitor de perfil, etc. y estos a su vez envían la información procesada al cuadro de mando el cual es el encargado de presentar visualmente los resultados según el orden en que vayan llegando ya sea esto en tiempo real o haciendo uso de la consola forense la cual muestra todos los eventos suscitados al momento de presentarse la alerta. Mediante el cuadro de mando se podrá visualizar el comportamiento de la red ya que este toma esta información de cada uno de los monitores.

2.6 Fase de optimización

Debido a que no se encontraron errores en la implementación del laboratorio se mantiene el diseño de la red planteado y se procederá posteriormente a su utilización y manipulación según las necesidades.

CAPÍTULO 3

PRUEBAS, DESARROLLO E INTEGRACIÓN

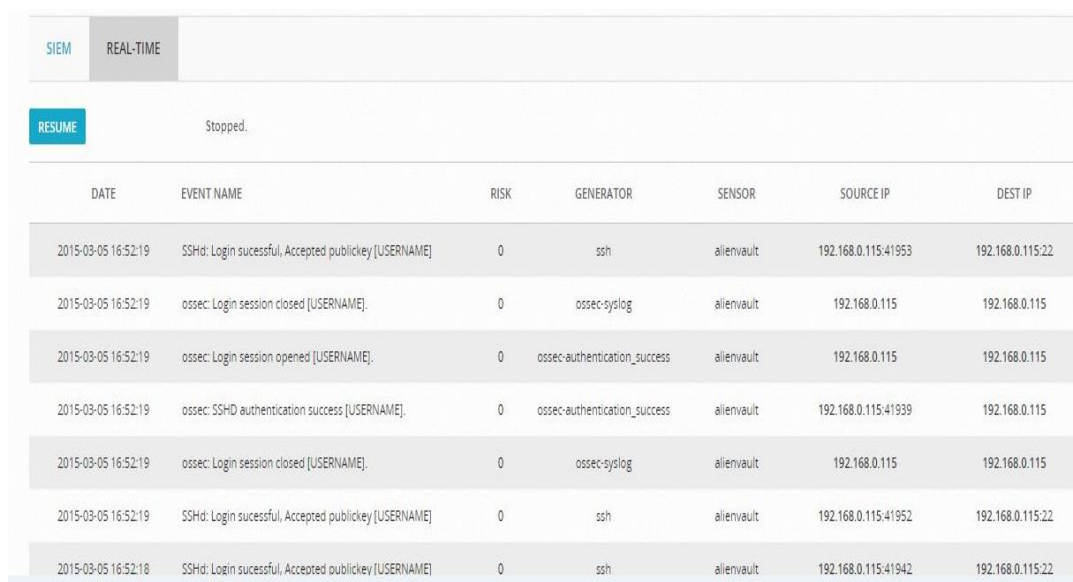
3.1 Pruebas

3.1.1 Herramientas de OSSIM.

- OSSEC

La configuración básica de esta herramienta es cargada automáticamente en la instalación de OSSIM, permitiendo visualizar la información de los sucesos de la red inmediatamente, pero para la detección de nuevos eventos se debe configurar nuevas reglas dependiendo la necesidad del administrador.

Visualizador de eventos SIEM



The screenshot shows the SIEM event viewer interface. At the top, there are two tabs: 'SIEM' (selected) and 'REAL-TIME'. Below the tabs, there is a 'RESUME' button and a status indicator 'Stopped.'. The main area contains a table with the following columns: DATE, EVENT NAME, RISK, GENERATOR, SENSOR, SOURCE IP, and DEST IP. The table displays several events, including SSH login successes and OSSEC session events.

DATE	EVENT NAME	RISK	GENERATOR	SENSOR	SOURCE IP	DEST IP
2015-03-05 16:52:19	SSHD: Login successful, Accepted publickey [USERNAME]	0	ssh	alienvault	192.168.0.115:41953	192.168.0.115:22
2015-03-05 16:52:19	ossec: Login session closed [USERNAME].	0	ossec-syslog	alienvault	192.168.0.115	192.168.0.115
2015-03-05 16:52:19	ossec: Login session opened [USERNAME].	0	ossec-authentication_success	alienvault	192.168.0.115	192.168.0.115
2015-03-05 16:52:19	ossec: SSHD authentication success [USERNAME].	0	ossec-authentication_success	alienvault	192.168.0.115:41939	192.168.0.115
2015-03-05 16:52:19	ossec: Login session closed [USERNAME].	0	ossec-syslog	alienvault	192.168.0.115	192.168.0.115
2015-03-05 16:52:19	SSHD: Login successful, Accepted publickey [USERNAME]	0	ssh	alienvault	192.168.0.115:41952	192.168.0.115:22
2015-03-05 16:52:18	SSHD: Login successful, Accepted publickey [USERNAME]	0	ssh	alienvault	192.168.0.115:41942	192.168.0.115:22

Figura 11. Panel de visualización, muestra la información obtenida por OSSEC

Fuente: OSSIM

La integridad de la información de un sistema informático es fundamental para mantener estable una entidad, la herramienta OSSEC ofrece la funcionalidad de monitorear los directorios que consideremos sensibles para el correcto funcionamiento del sistema. Este tipo de monitoreo se lo debe configurar tanto en los agentes previamente instalados en los equipos a monitorear como en el servidor, lo cual se lo realizará de la siguiente forma:

Ingresa en la consola de un agente en el archivo de configuración ossec.conf el cual se encuentra en la ruta “/var/ossec/etc/”, se debe localizar la etiqueta <syscheck> y dentro de los parámetros de esta etiqueta aumentaremos las siguientes líneas:

Código fuente:

```
<alert_new_files>yes</alert_new_files>
<directories report_changes="yes" realtime="yes"
check_all="yes">/home/prueba</directories>
```

La información generará una alerta al momento en que se vea afectada la integridad de algún archivo o directorio dentro de la ruta especificada en la etiqueta <directories> en este caso /home/prueba pudiendo ser esta cualquier tipo de directorio ya sea en un equipo con sistema Windows, Linux o Mac, teniendo algunos parámetros dentro de la etiqueta para que esto sea verificado en tiempo real en todos los archivos pertenecientes a este directorio.

Para complementar esta configuración se debe agregar en una nueva regla en el archivo de configuración local_rules.xml el cual se encuentra en la ruta del servidor OSSIM “/var/ossec/rules” y se incrementarán las siguientes líneas:

Código fuente:

```
<rule id="554" level="7" overwrite="yes">
<category>ossec</category>
<decoded_as>syscheck_new_entry</decoded_as>
<description>File added to the system.</description>
<group>syscheck,</group>
</rule>
```

En la regla que se encuentra en el archivo en el archivo ossec_rules.xml que tiene un nivel 0, que impide que se notifiquen los cambios hechos por ser una alerta de bajo nivel y es por esta razón que se debe sobre escribir con un nivel 7, mediante el comando overwrite=”yes” colocado en la etiqueta de la regla agregada en local_rules.xml. Para concretar los cambios en las configuraciones se debe reiniciar el servicio de ossec en el servidor y agente configurado.

Nuevo manejador de evento de OSSEC



Figura 12. Evento OSSEC de adición de archivo en directorio

Fuente: OSSIM

Posteriormente realizadas las pruebas y nuevas configuraciones a la herramienta integrada OSSEC, se realizó un análisis encontrando que existen tiempos altos en la obtención de información de los eventos.

Localizado el problema es necesario redistribuir la información, clasificando los archivos por el tipo de log, con esto se obtendrá mejores tiempos de respuesta en la administración.

- **NMAP**

La configuración de NMAP se encuentra cargada automáticamente en OSSIM, permitiendo realizar el descubrimiento de los equipos activos que se encuentren en la red.

Descubrimiento de activos Nmap

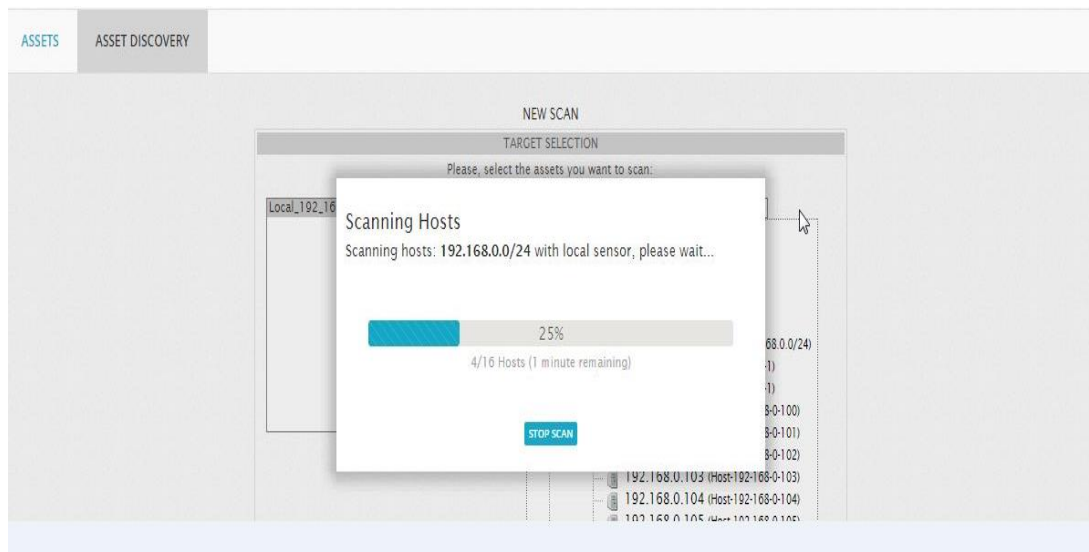


Figura 13. Escaneo de activos de red mediante herramienta NMAP

Fuente: OSSIM

Al realizar el descubrimiento de los host de red, se puede visualizar la información respectiva a cada equipo IP address, hostname, MAC address, Sistema Operativo y los servicios que se encuentran activos.

Lista de equipos activos

SCAN RESULTS							
<input checked="" type="checkbox"/>	HOST	HOSTNAME ^(?)	FQDN	DEVICE TYPES	MAC ^(?)	OS ^(?)	SERVICES ^(?)
<input checked="" type="checkbox"/>	192.168.0.1	Host-192-168-0-1	-	General Purpose	C8:3A:35:36:B5:C8	? VxWorks	http
<input checked="" type="checkbox"/>	192.168.0.103	Host-192-168-0-103	-	General Purpose	00:23:8B:89:39:AC	Windows/7	msrpc, netbios-ssn, netbios-ssn, ms-wbt-server
<input checked="" type="checkbox"/>	192.168.0.105	Host-192-168-0-105	-	General Purpose	00:08:54:34:40:9A	Linux/2.6.X	ssh, http, http-ssl
<input checked="" type="checkbox"/>	192.168.0.106	Host-192-168-0-106	-	General Purpose	00:8C:FA:3C:DE:8D	Windows/Vista	smtp, http, msrpc, netbios-ssn, http-ssl, netbios-ssn

Figura 14. Listado de activos descubiertos mediante escaneo NMAP

Fuente: OSSIM

Posteriormente realizadas las pruebas con el descubrimiento de equipos no se encontró observación alguna, ya que la herramienta funciona en forma óptima al ser integrada en OSSIM.

- **NAGIOS**

Herramienta que se encarga de mostrar los servicios activos en los equipos pertenecientes a la red. Una vez agregados los equipos a las configuraciones de NAGIOS mostrará el estado de cada servicio, mediante la descripción “UP” y un recuadro de color verde cuando los servicios se encuentran arriba sin inconveniente o un “DOWN” si alguno de los servicios está abajo, lo que sería un indicativo de que un agente externo o interno ingresó y causó la desactivación del servicio en el sistema, entre los servicios que monitorea NAGIOS tenemos los siguientes:

- Carga actual
- Usuarios actuales
- Espacio de disco
- Servicio HTTP
- Servicio ICMP
- Servicio SSH

Para agregar los equipos a la consola de NAGIOS es necesario realizar las siguientes configuraciones para cada equipo que se encuentra activo en la red:

- **Registro de host**

En el registro de un host se debe crear un archivo, el cual, define la información del host con la extensión “.cfg” en la ruta /etc/nagios3/conf.d, el mismo que debe contener las siguientes líneas de código:

Código fuente:

```
define host{
usegeneric-host ;      Nombre de la plantilla genérica
host_name              NOMBRE_DEL_HOST
alias                  ALIAS_HOST
address                IP_HOST
}
```

- **Definición de servicios**

En cada host registrado se debe definir los servicios que van a ser monitoreados para lo cual se utilizará una plantilla en la que están definidos los servicios a monitorear. Para que NAGIOS pueda verificar el estado de los servicios se agrega las líneas de código al archivo creado para el registro del host en la consola de NAGIOS, la información se agregara dependiendo el servicio que se necesite monitorear:

Código fuente:

```
Define service{
use                generic-service ; Nombre de la plantilla de servicios
host_name          NOMBRE_DEL_HOST
service_description NOMBRE_DEL_SERVICIO
check_command       COMANDO_DE_MONITOREO
}
```

- **Definición de grupos**

La herramienta NAGIOS nos permite clasificar y agrupar los host basándose en múltiples variables, como son: el tipo de servicios que posee cada dispositivo, el sistema operativo que tiene instalado, entre otros.

Para que la herramienta muestre los host organizados grupalmente en la consola administrativa es necesario definir los grupos con las siguientes líneas de código en el archivo `hostgroups_nagios2.cfg` de la siguiente forma:

Código fuente:

```
Define hostgroup {
hostgroup_name      NOMBRE_DEL_GRUPO
alias               ALIAS_DEL_GRUPO
members             MIEMBROS_DEL_GRUPO
}
```

El nombre del grupo debe constar en el archivo `extinfo_nagios2.cfg` en caso de tratarse de un grupo clasificado por S.O, en caso de tratarse de grupos definidos por servicios prestados el nombre de estos deberán constar en el archivo `services_nagios2.cfg` para su correcto funcionamiento.

En la línea de código número 4 que precede a la variable “members” se debe colocar el o los nombres de los dispositivos que pertenecerán a este grupo, siendo necesario que cada uno de estos tenga el nombre que se le asignó en el registro de host deben estar separados por una coma uno del otro. Una vez registrado cada host en los archivos de configuración de NAGIOS y definido cada una de las configuraciones anteriores la consola administrativa mostrará en pantalla los dispositivos virtuales agregados y el estado de los servicios.

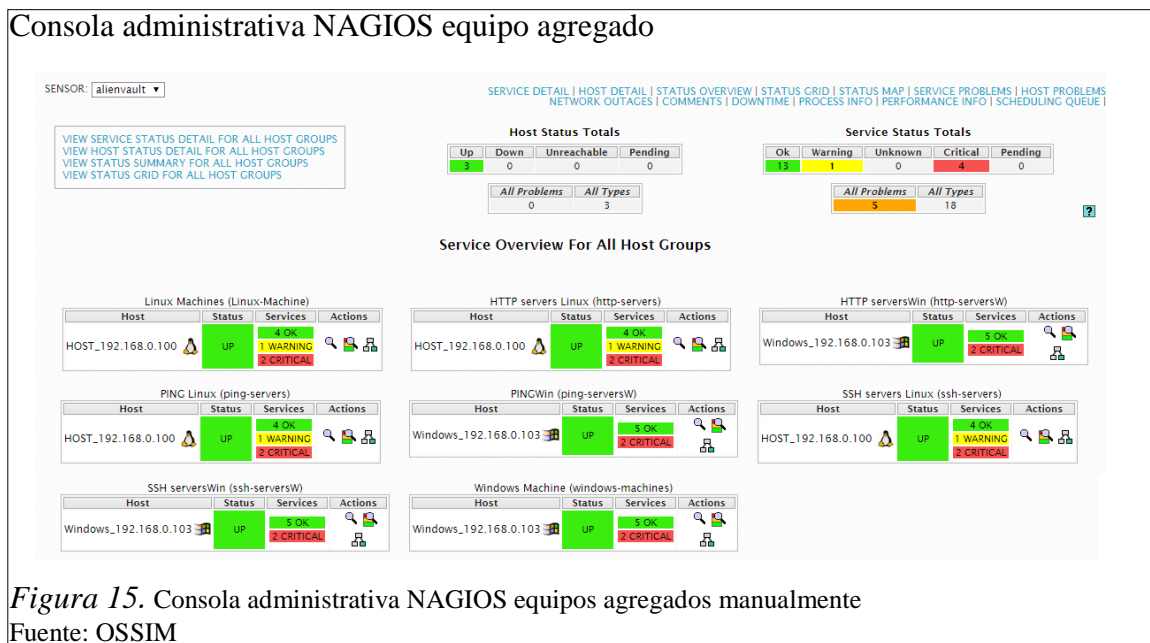


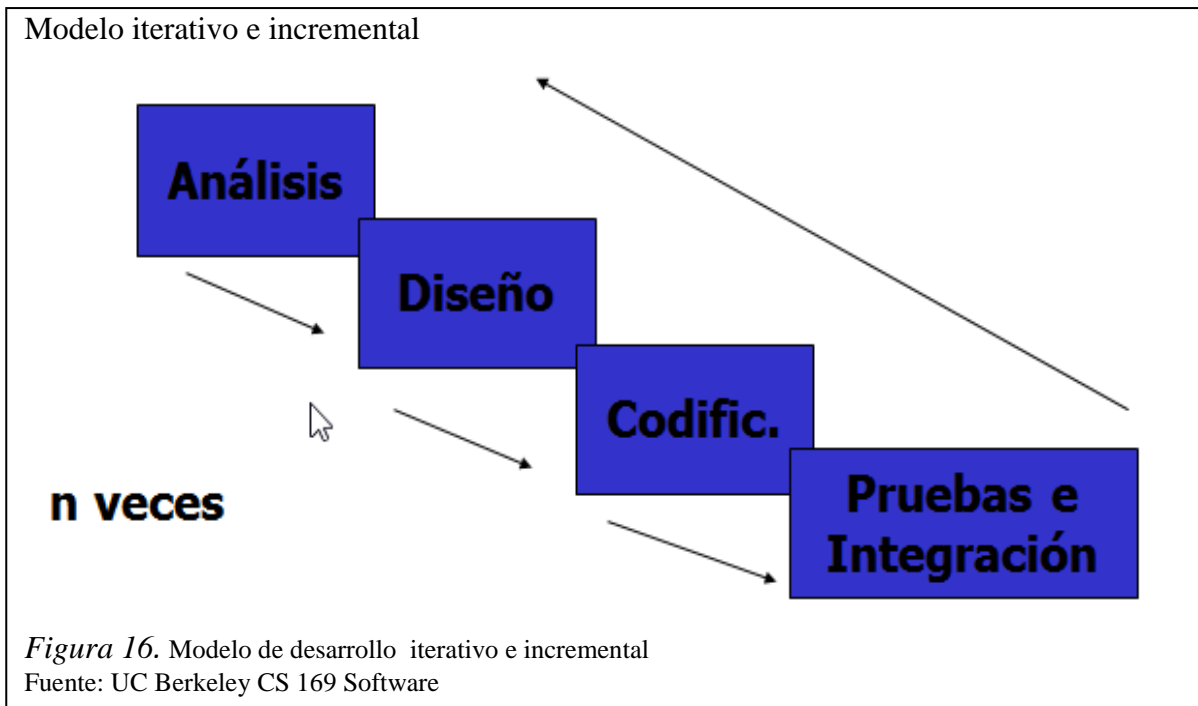
Figura 15. Consola administrativa NAGIOS equipos agregados manualmente

Fuente: OSSIM

Posteriormente realizadas las pruebas y configuraciones a la herramienta integrada NAGIOS se encontró que existe tiempos altos en la configuración e ingreso de los host para que puedan ser visualizados en la consola administrativa, siendo esto un limitante para el administrador.

3.2 Desarrollo

El siguiente desarrollo e implementación se realizó basado en el modelo de desarrollo iterativo e incremental, este tipo de programación consiste en la realización de programas de manera incremental, ya que sirve para obtener ventaja de lo que se ha realizado a lo largo del proyecto con lo cual se llega a obtener una nueva versión del sistema.



Después de realizadas las pruebas en el laboratorio del funcionamiento de las herramientas más significativas y esenciales de OSSIM, se encontró los siguientes necesidades para aumentar el rendimiento de la herramienta.

Tabla 15. *Descripción de las soluciones*

Herramienta	Soluciones planteada
OSSEC	Redireccionar los archivos de configuración y modificación del código fuente.
NAGIOS	Generar un gestor que permita el ingreso automático de los host que se encuentran activos en la red.

Nota. Descripción de las soluciones a adoptar en el sistema
Elaborado por: Diego Poveda & Alexis Balarezo

3.2.1 Soluciones de tiempos de respuesta en OSSEC

El problema en el retraso para la obtención de información de las herramientas de monitoreo es muy común, las principales casusas de esta situación es que toda la información se envía a un solo archivo, el cual, contiene los datos por evento generados

de la red que son recolectados en este caso por OSSEC. Para solventar el inconveniente se procederá al análisis de código de extracción de la información.

- **Redireccionar la información**

Para obtener la información de los eventos y que estos datos sean normalizados por OSSIM se cuenta con una variedad de plugins que son archivos de configuración para cada herramienta del sistema, para obtener tiempos de respuesta apropiados en la obtención de información se debe seleccionar y organizar la información que es recolectada de los agentes por el servidor, para que estos datos sean desplegados en la consola del OSSIM en forma óptima.

Debido a que la herramienta OSSEC cuenta con varios servicios integrados a monitorear, el tiempo de respuesta para el envío de notificaciones a la consola administrativa se torna lento, para lo cual se agilizará la carga de las notificaciones del servicio SSH de la siguiente manera:

Objetivo: Configurar host a monitorear.

Conectar directamente al servidor OSSIM para enviar los logs generados.

Código fuente:

```
[root@localhost rsyslog.d]# pwd
/etc/rsyslog.d

[root@localhost rsyslog.d]# vi alienvault.conf
*.* @192.168.0.115
```

Implementación:

En cada uno de los equipos a ser monitoreado los cuales cuenten con el servicio de SSH se deberá configurar el envío de los logs generados con destino hacia el servidor AlienVault OSSIM, lo cual se lo realiza con la creación de un archivo con el nombre referente al uso que se le va a dar y con extensión “.conf” en la ruta del sistema rápido de procesamiento de registros “/etc/rsyslog.d”.En el archivo creado se deberá agregar la línea de código de conexión “*.*

@IP_SERVIDOR” la que indica que se enviará al servidor todos los logs generados en el equipo. Es necesario el reinicio del servicio rsyslog.

Se necesita una regla para realizar el filtrado de logs de cada equipo a escuchar que contengan rastros SSH.

Objetivo: Creación de regla para filtrar logs OSSEC-SSH.

Se creará una regla para filtrar logs de equipos a escuchar que contengan rastros SSH.

Código fuente:

```
if ($fromhost-ip startswith '192.') and ($rawmsg contains 'ssh') then /var/log/ssh-remote.log  
& ~
```

Implementación:

Una vez configurado cada host a monitorear se procede con las configuraciones en el servidor, comenzando con la creación del archivo en la ruta del sistema rápido de procesamiento de registros “rsyslog”, el que se encargará de escuchar los eventos generados en cada cliente que para el caso tendrá el mismo nombre que el plugin del servicio “ssh-remote” con extensión “.conf” en donde se agregará la línea de código con las condiciones a escuchar de la siguiente forma:

```
“if($fromhost-ipstartswith 'RED_A_ESCUCHAR') and ($rawmsgcontains  
'CONTENIDO_DEL_LOG') then  
RUTA_Y_NOMBRE_ARCHIVO_LOG_ALMACENAMIENTO& ~”.
```

Crear un archivo que almacena los logs generados el cual contenga las especificaciones del archivo de configuración.

Objetivo: Crear archivo de almacenamiento de logs generados.

Se agregará un archivo que almacene los logs generados que contengan las especificaciones del archivo de configuración.

Código fuente:

```
alienvault:/var/log# touch ssh-remote.log

alienvault:/var/log# ls -ltr ssh-remote.log
-rw-r--r-- 1 root root 557098 Mar  7 10:48 ssh-remote.log
```

Implementación:

Una vez creado el archivo de configuración que escucha los eventos de los equipos se debe crear el archivo que contendrá los logs capturados, siendo este equivalente al que se menciona en la línea de código colocada en el archivo de configuración, teniendo en cuenta que debe estar en la misma ruta especificada.

Configurar el plugin para que se relacione con el archivo que almacena los logs generados por los equipos de la red.

Objetivo: Establecer conexión plugin-log.

Se configurará el plugin para que esté relacionado con el archivo donde se almacenarán los logs generados.

Código Fuente:

```
[config]
type=detector
enable=yes

source=remote-log
location=/var/log/ssh-remote.log
```

Implementación:

Una vez creado se debe configurar el plugin, para que este se conecte con el archivo que almacena la información de logs generados, se debe cambiar únicamente las líneas “source= log”, “location=/var/log/auth.log” colocando: “source=remote-log”, “location=/var/log/ssh-remote.log” y procedemos a reiniciar el servicio de ossim-agent.

Agregar la ruta y nombre del archivo de almacenamiento de logs creado para que sea leído por el sistema.

Objetivo: Legibilidad a archivo de logs.

Se debe agregar la ruta y nombre del archivo de almacenamiento de logs creado para que sea leído por el sistema.

Código fuente:

```
/var/log/cron.log
/var/log/debug
/var/log/messages
/var/log/ssh-remote.log
{
    rotate 4
    weekly
    missingok
    notifempty
    compress
    delaycompress
    sharedscripts
    postrotate
        invoke-rd.d rsyslog reload > /dev/null
    endscript
}
```

Implementación:

Se procede a la agregación de la ruta y el nombre del archivo “/var/log/ssh-remote.log” en donde se alojará la información de los logs en el archivo de rotación “/etc/logrotate.d/rsyslog” se procede a forzar la rotación con el comando “logrotate -f /etc/logrotate.d/rsyslog”, para que el sistema empiece a leer. Al destinar un archivo que escuchará los logs que contengan SSH se logra optimizar el tiempo ya que el destino será únicamente para este tipo de logs.

- **Reglas para visualizar la información.**

Para visualizar la información en forma detalla y realizando un análisis de las normas utilizadas en PCI e ISO, se procede a crear reglas de seguridad las cuales están basadas

en la autenticación de usuarios, todo esto se logra mediante la información que se solicita al usuario para que se valide su acceso. Se debe recordar que las reglas pueden ser creadas dependiendo la necesidad del administrador, para la siguiente investigación se procederá a crear dos reglas, ya que el estudio y análisis de las mismas no se encuentra estipulado en el presente documento.

Objetivo: Reglas para múltiples accesos fallidos y usuario invalido.

- La información tanto del host de origen que intenta realizar un acceso no autorizado y el host de destino al que el acceso está dirigido se visualicen como una incidencia, la cual, pueda ser analizada por el administrador para la identificación del problema.
- La información del usuario que desea ingresar sea la correcto caso contrario se creará la incidencia.



Figura17. Muestra las reglas creadas para la autenticación de los usuarios
Fuente: OSSIM

3.2.2 Gestor de integración de datos para NAGIOS

NAGIOS es una de las herramientas de monitoreo de servicios de red más poderosas que se tiene en la actualidad, pero el proceso de ingreso de cada host, servicios y grupos a los que perteneces, se realiza mediante la configuración de los archivos internos de NAGIOS en forma manual, es una gran desventaja al momento de monitorear y obtener información de un determinado equipo puesto que los tiempo de configuración son sumamente altos dependiendo la extensión de la red, esta necesidad permite que en la presente investigación se proceda a generar un Gestor para la información de cada host en NAGIOS.

El Gestor de host NAGIOS, permite integrar dos de las herramientas más poderosas e importantes que se encuentra integradas en OSSIM, las cuales, por la forma de presentar la información permiten que se relacionen los datos, estas son NMAP y lógicamente NAGIOS, las funcionalidades de estas herramientas fueron descritas en apartados anteriores.

En el siguiente apartado se muestra el código fuente que es generado e implementado para el Gestor de información NAGIOS, se debe mencionar que se detallará y publicará el código y configuraciones que se consideren más importante y que permiten alcanzar el objetivo principal, ya que no es necesario describir las líneas de código conocidas.

Se necesita obtener la máscara de subred para determinar el número de host que serán escaneados.

Objetivo: Obtener la información de la red.

Obtener la máscara de subred para determinar el número de host.

Código fuente:

```
mascara=`netstat -r |grep localnet| awk '{ print $3 }'`  
octmasc4=`echo $mascara|awk -F "." '{print $4}'`  
  
octeto1=`ip a | grep inet| awk '{ print $2 }'| awk -F "127.0.0.1/8" '{ print $1 }'| awk -F "/" '{ print $1 }'| aw  
octeto2=`ip a | grep inet| awk '{ print $2 }'| awk -F "127.0.0.1/8" '{ print $1 }'| awk -F "/" '{ print $1 }'| aw  
octeto3=`ip a | grep inet| awk '{ print $2 }'| awk -F "127.0.0.1/8" '{ print $1 }'| awk -F "/" '{ print $1 }'| aw  
octeto4=`ip a | grep inet| awk '{ print $2 }'| awk -F "127.0.0.1/8" '{ print $1 }'| awk -F "/" '{ print $1 }'| aw
```

Es necesaria la comparación del cuarto octeto de la máscara de red para obtener el número total de host de la red y compararlo con el cuarto octeto de la IP local para obtener la dirección IP de red mediante la operación AND y poder empezar el escaneo de la red.

Objetivo: Comparar el número de host a escanear.

Comparación del cuarto octeto de mascara de red para obtener el número total de host y la dirección de ip de red para empezar el escaneo. (Larador, 2015, págs. 33-36).

Código fuente:

```
if [[ $oct Masc4 = 0 ]]; then
    expo=8
else
    expo=`echo "obase=2;$oct Masc4" | bc |grep -oh 0|grep -c 0`
fi
hostnum=$((2**$expo))
octetored=$(( $oct Masc4 & $octeto4 ))
inicio=$(( $octetored + 1 ))
fin=$(( $octetored + $hostnum -1 ))
rango=$inicio
while [[ $rango -le $fin ]]; do
    IP=$octeto1.$octeto2.$octeto3.$rango
    if ping $IP -w 3 -c 1 > /dev/null; then
        if [[ $inactivo -eq 1 ]]; then
            echo ""
        fi
    fi
done
```

Es necesario verificar el sistema operativo correspondiente a cada host para clasificar si es Linux, Windows u otro sistema, mediante este parámetro crear grupos en NAGIOS.

Objetivo: Información del sistema operativo mediante NMAP.

Verificar el sistema operativo correspondiente a cada host para clasificar si es Linux, Windows u otro para la creación de grupos en NAGIOS.

Código fuente:

```
SOCLOUD=`nmap -O $IP | grep "Running:" |sed s/Running://|sed s/Microsoft//|awk '{ print $1 }'`

if [[ -z $SOCLOUD ]]; then
    SOCLOUD="HOST"
fi
```

Se necesita identificar si cada host de la red se encuentra registrado en la configuración de NAGIOS para que no sea duplicado en la consola administrativa.

Objetivo: Verificación de equipos.

Si el equipo ya se encuentra registrado no vuelve a crear el archivo de configuración para el host y que este no sea duplicado en la consola de NAGIOS.

Código fuente:

```
cd /etc/nagios3/conf.d/
existe=`find $SOCLOUD`_'$IP.cfg`
echo $IP $mac activo

if [[ ! -z $existe ]];then
    echo "Equipo ya registrado"
else
    /etc/nagios3/conf.d/plantilla $IP $SOCLOUD
fi
echo ""
eqpas=0
contarin=0
```

Es necesario verificar conectividad con todos los host de la red e identificar si la ip está activa o inactiva, aplicando parámetros de inactividad a través un rango de 10 host inactivos empleando un salto al siguiente grupo de host.

Objetivo: Respuesta de los host por ICMP.

Se verifica respuesta de los host mediante el ICMP al existir conexión se declara al equipo como pasivo, para que no sea ingresado en la configuración de NAGIOS. (Mike, 2014, págs. 10-11).

Código fuente:

```
else
if [[ $eqpas -eq 1 ]] ; then
    contarin=$((contarin+1))
if [[ $contarin -eq 10 ]]; then
if [[ $rango -le 50 ]]; then
rango=49
contarin=0
elif [[ $rango -le 100 ]]; then
rango=99
contarin=0
```

```

elif [[ $rango -le 150 ]]; then
rango=149
contarin=0
elif [[ $rango -le 200 ]]; then
rango=199
contarin=0
elif [[ $rango -le 250 ]]; then
rango=$fin
contarin=0
fi
fi
echo -en "\e[1A"
echo "$IP pasivo";
else
echo "$IP pasivo";
eqpas=1
fi
fi
rango=$(( $rango+1 ))
done

```

Para el monitoreo de cada host NAGIOS necesita el archivo de configuración donde se detalla los parámetros de cada host y los servicios a monitorear.

Objetivo: Crear el archivo para definir el host, los servicios y grupos.

Recibe toda la información de los host que se encuentran activos y que serán registrados e ingresados en NAGIOS para su publicación en la consola.

Código fuente:

```

IP=$1
SOCloud=$2
Wn="Windows"
Ln="Linux"
touch /etc/nagios3/conf.d/$SOCloud_"$IP.cfg
chmod 777 /etc/nagios3/conf.d/$SOCloud_"$IP.cfg
echo "define host{
    use generic-host ; Name of host template to use
    host_name $SOCloud_"$IP
    alias host.$IP
    address $IP
}

define service{
    use generic-service ; Name of service template to use
    host_name $SOCloud_"$IP
    service_description Disk Space
    check_command check_all_disks!20%!10%
}

define service{
    use generic-service ; Name of service template to use
    host_name $SOCloud_"$IP
    service_description Current Users
    check_command check_users!20!50
}

```

Cada host configurado en la consola de NAGIOS necesita ser asignado a un determinado grupo para realizar su administración.

Objetivo: Asignación de host a cada grupo.

Envío de información dependiendo al grupo de servicios que se desee añadir.

Código fuente:

```
if [[ $SOCLOUD = $Wn ]]; then
    sed -i '/members/ s/members/members '$SOCLOUD'_"$IP","/g' /etc/nagios3/conf.d/hostgroups_nagios2.cfg
elif [[ $SOCLOUD = $Ln ]]; then
    sed -i '/members/ s/members/members '$SOCLOUD'_"$IP","/g' /etc/nagios3/conf.d/hostgroups_nagios1.cfg
else
    sed -i '/members/ s/members/members '$SOCLOUD'_"$IP","/g' /etc/nagios3/conf.d/hostgroups_nagios1.cfg
fi
```

Integración

Para que el Gestor se ejecute al inicial el sistema de OSSIM se debe ingresar en el archivo rc.local la dirección que aloja al script.

```
#!/bin/bash
# Set interfaces eth0
ifconfig eth0 up
ifconfig eth0 promisc
ethtool -G eth0 rx 4096 tx 4096
ethtool -K eth0 gro off
echo deadline > /sys/block/sda/queue/scheduler
sh /etc/ossim/server/autodetection.sh
```

CAPÍTULO 4

PRUEBAS

4.1 Pruebas funcionales Cloud Computing

Las pruebas funcionales permiten y tienen como objetivo la visualización de los resultados en la manipulación de la aplicación, permiten identificar inconsistencias y las posibles soluciones.

Tabla 16. *Pruebas de funcionalidad de la Cloud Computing (XenServer)*

N.	Objetivo	Secuencia	OK	Resultados
1	Verificar Conexión	1PING nodo máster 2 PING nodo1 3 PING nodo2 4 PING VM 1 5 PING VM 2	SI	
2	Administrar Nodos	1 Ingresar nodo máster 2 Ingresar nodo 1 3 Ingresar nodo 2	SI	
3	Acceder VM Clientes	1 Acceso nodo 1 2 Ingresar a la VM 1 3 Acceso nodo 2 4 Ingresar a la VM 2	SI	
4	Migrar VM 1, 2 al nodo máster	1 Acceder al nodo 1 2 Migrar VM 1 al nodo máster 3 Acceder al nodo 2 4Migrar VM 2 a nodo máster	SI	VM 1, 2 migradas al nodo máster
5	Migrar VM entre nodos 1, 2	1 Acceder al nodo 1 2Migrar VM 1 al nodo 2 3 Acceder al nodo 2 4 Migrar VM 2 a nodo 1	SI	VM 1, 2 migradas ente nodo 1 y nodo 2
6	HA VM 1 al nodo 2	1 Acceder al nodo 1 2 Apagar nodo 1	SI	VM1 conmuta al nodo 1
7	HA VM 2 al nodo 1	1 Acceder al nodo 2 2 Apagar nodo 2	SI	VM2 conmuta al nodo 1
8	HA VM 1, 2 al nodo máster	1 Acceder al nodo 1 2 Apagar nodo 1 3 Acceder al nodo 2 4 Apagar nodo 2	SI	VM conmutan al nodo máster

Nota. Descripción de la funcionalidad de la Cloud Computing

Elaborado por: Diego Poveda & Alexis Balarezo

- **Carga**

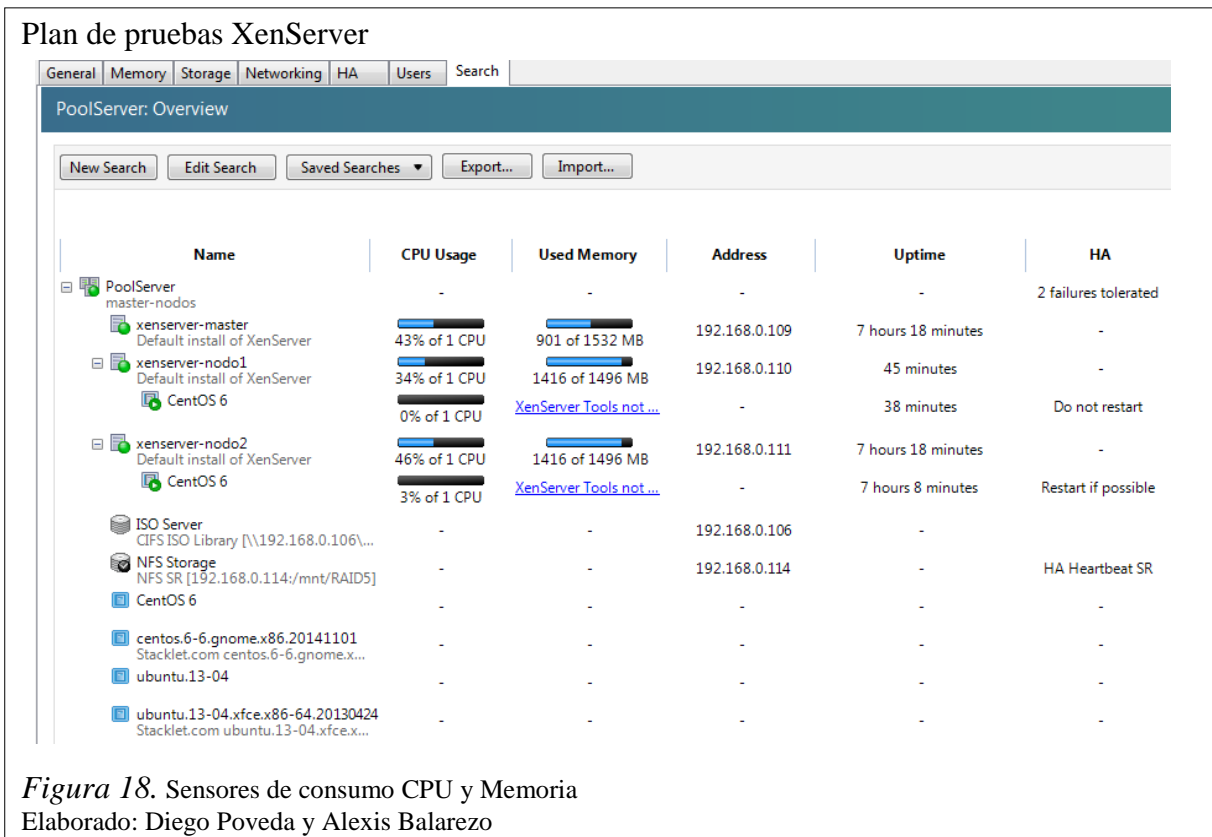
Estas pruebas están diseñadas para verificar el comportamiento del sistema Cloud y sus respectivos nodos frente a la indisponibilidad de alguno de estos, el proceso consiste en hacer que el nodo máster reciba las VM en caso de fallo de un nodo secundario.

Para la mencionada prueba se ha configura y activado los sensores implementados en XenServer que permite realizar un monitoreo del rendimiento del sistema.

Tabla 17. *Abreviaturas para la prueba de funcionalidad de la Cloud Computing.*

Abreviaturas	Descripción	Abreviaturas	Descripción
CPUI	Consumo Inicial del CPU	UMI	Uso de la memoria inicial
CPUC	Consumo Conmutación del CPU	UMC	Uso de la memoria en la conmutación
CPUF	Consumo Final del CPU	UMF	Uso de la memoria final

Nota. Descripción de las abreviaturas para las pruebas funcionales de la Cloud Computing
Elaborado por: Diego Poveda & Alexis Balarezo



- **Análisis**

El sistema del nodo máster se encuentra configurado para soportar las máquinas que se encuentren en el nodo 1 y nodo 2, por lo que se decidió realizar una carga al nodo máster de un 50% y otra carga con el 100% de pérdida de los nodos secundarios.

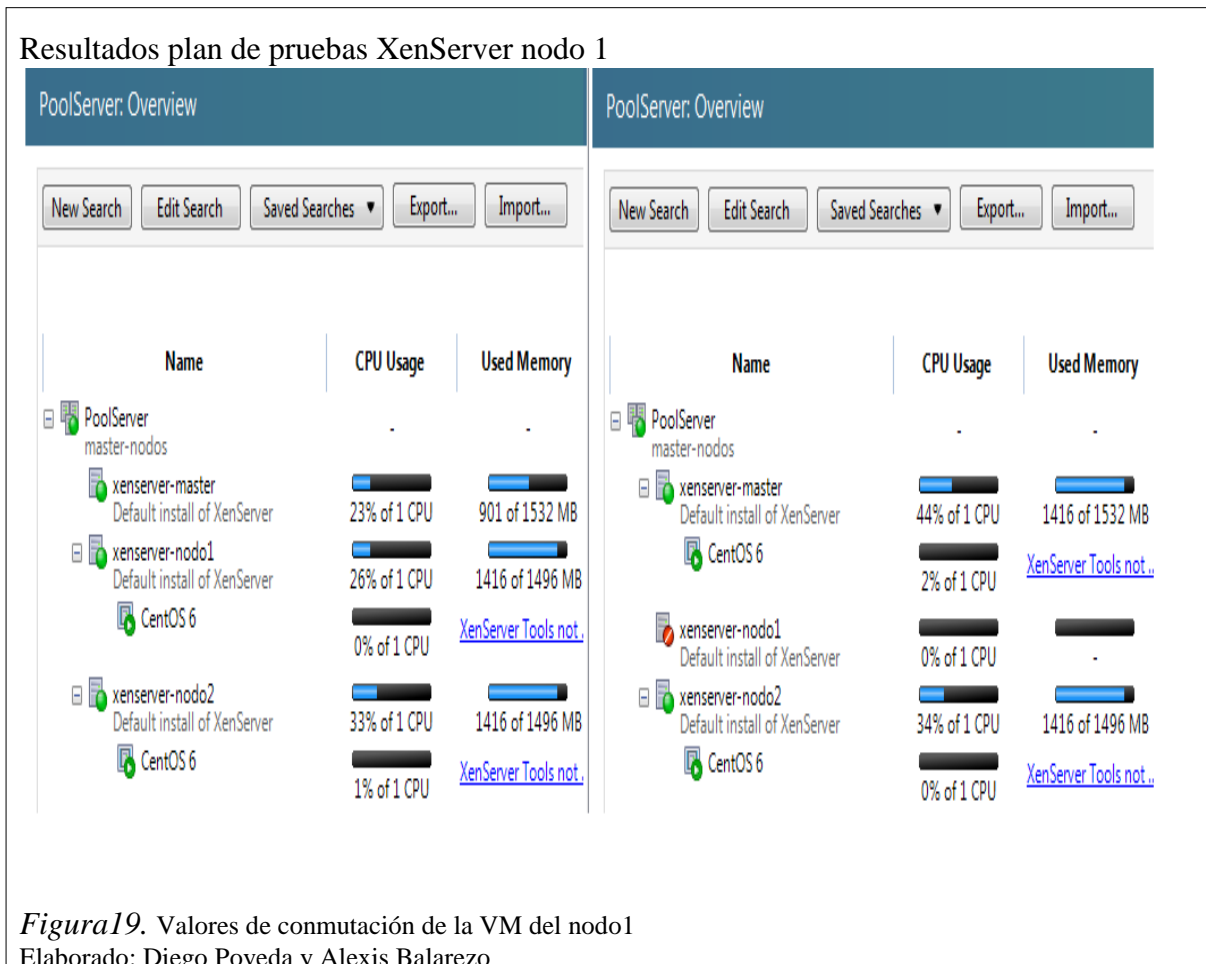


Tabla 18. *Resultados obtenidos, nodo 1*

Nodo	CPUI%	CPUC %	CPUF %	UMI(MB)	UMC(MB)	UMF(MB)
xenserver-nodo1	23	44	25	901	1416	1416

Nota. Descripción de resultados obtenidos en el nodo uno
Elaborado por: Diego Poveda & Alexis Balarezo

Se puede apreciar que le porcentaje al realizar la conmutación por fallo del nodo 1 es del 44% y el uso de memoria aumenta de 901MB a 1416MB pero al concluir la migración la carga de CPU regresa al rango normal de 25%.

Con la información obtenida se puede concluir que al activar la HA por fallo del nodo 1 el nodo máster aumenta el consumo de CPU en un 47% y el espacio de memoria del nodo máster es equivalente al de la máquina virtual está siendo utilizada.

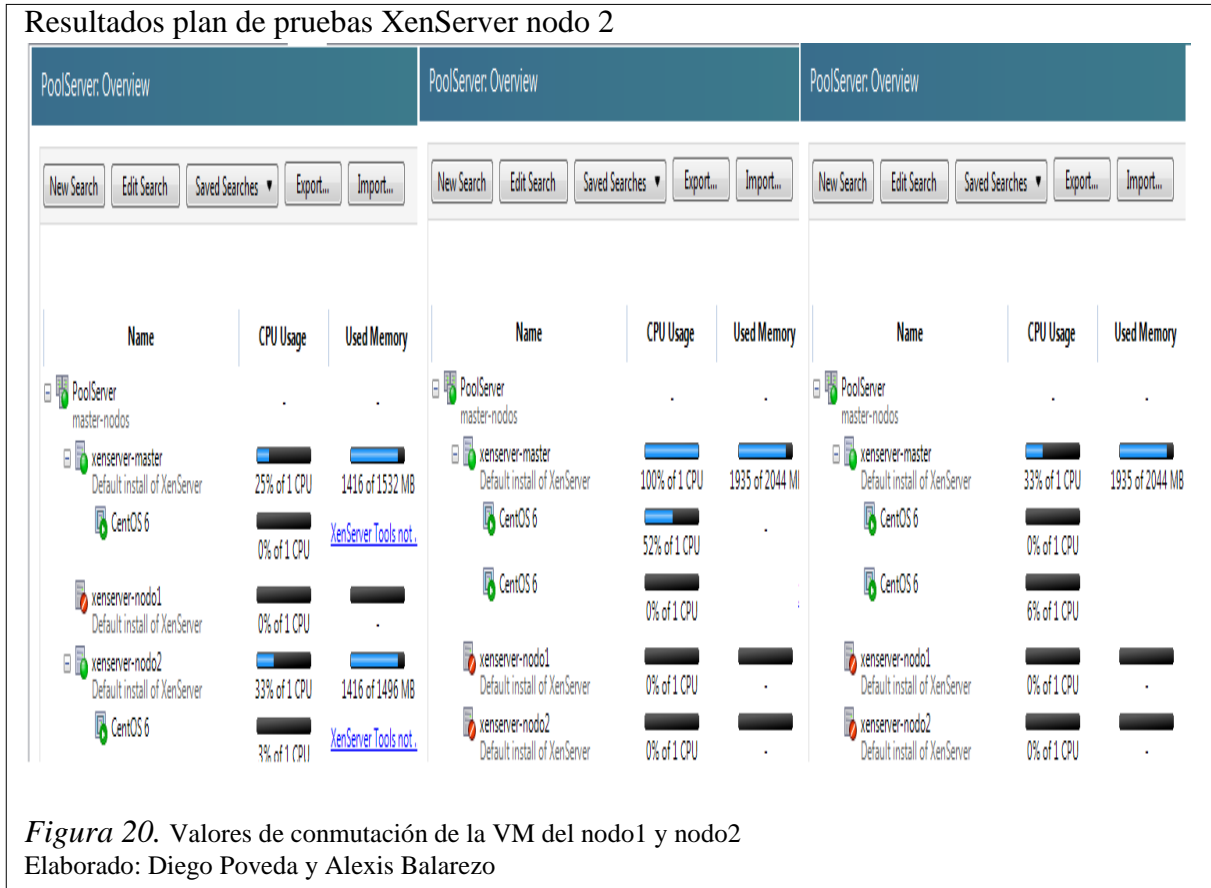


Tabla 19. Resultados obtenidos, nodo 2

Nodo	CPUI%	CPUC %	CPUF %	UMI(MB)	UMC(MB)	UMF(MB)
xenserver-nodo2	25	100	33	1436	1915	1915

Nota. Descripción de resultados obtenidos en el nodo dos
Elaborado por: Diego Poveda & Alexis Balarezo

Se puede apreciar que el porcentaje al realizar la conmutación por fallo del nodo 2 teniendo en cuenta que el nodo 1 se encuentra alojado en el nodo máster es del 100% y el uso de memoria aumenta de 1436MB a 1915MB pero al concluir la migración la carga de CPU regresa al rango normal de 33%.

Con la información obtenida se puede concluir que al activar la HA por fallo del nodo 2 el nodo máster aumenta el consumo de CPU en un 75% y el espacio de memoria del nodo máster es equivalente al de la máquina virtual está siendo utilizada.

- **Gráfica**

En la siguiente ilustración se muestran los resultados previamente obtenidos en forma gráfica, el que se puede apreciar la carga de CPU y la utilización de memoria del nodo máster en color azul y naranja respectivamente después de aplicar la conmutación de los nodos secundarios.

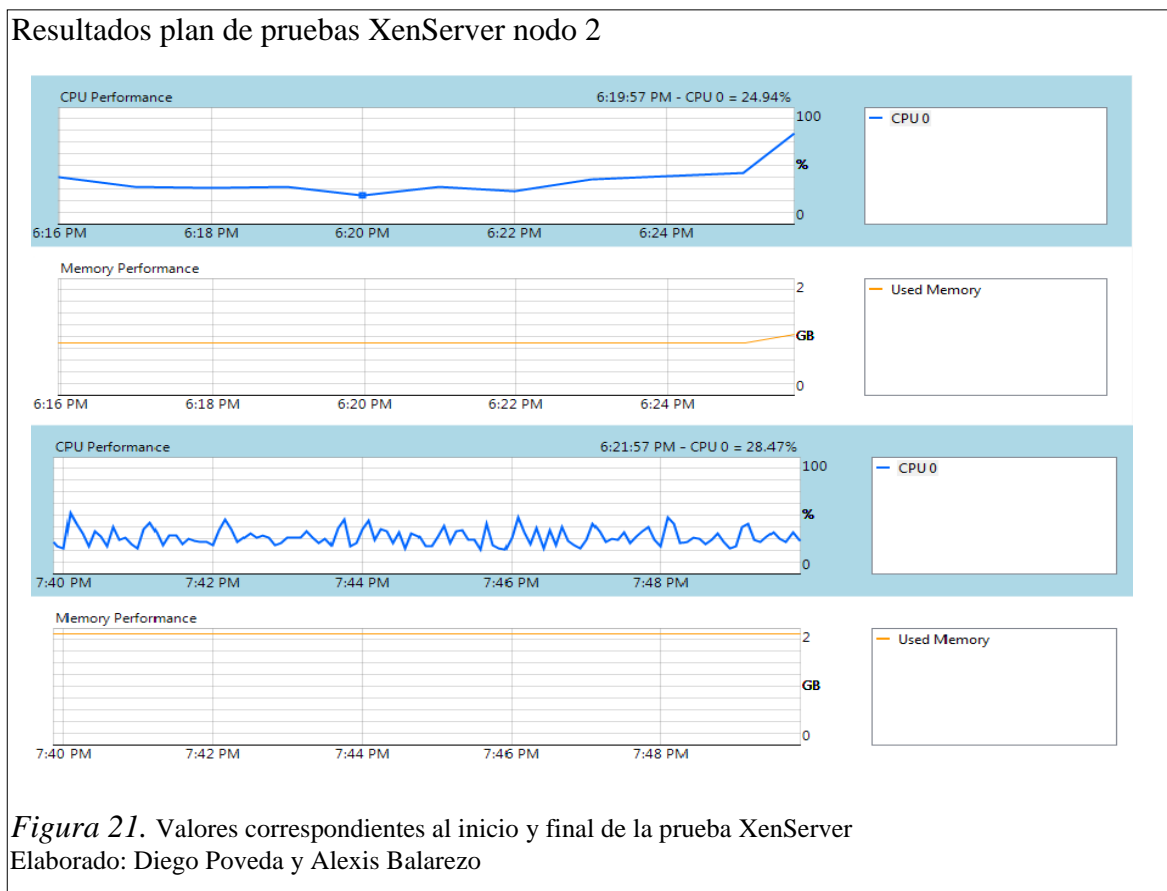


Tabla 20. Resultados obtenidos, nodo máster

Nodo	CPUI%	CPUF %	UMI(MB)	UMF(MB)
xenserver-nodo2	25	29	901	1915

Nota. Descripción de resultados obtenidos en el nodo máster
Elaborado por: Diego Poveda & Alexis Balarezo

4.2 Pruebas funcionales NAGIOS

Las pruebas funcionales permiten y tienen como objetivo principal la visualización de los resultados obtenidos al implementar los cambios en el código fuente y la automatización de los procesos de las herramientas anteriormente mencionadas, mediante estas evaluaciones se puede identificar inconsistencias y las soluciones.

Tabla 21. *Pruebas de funcionalidad Generador de host NAGIOS*

N.	Objetivo	Resultados	OK
1	Máscara de red	<pre>++ greplocalnet ++ netstat -r ++ awk '{ print \$3 }' + mascara=255.255.255.0 ++ awk -F . '{print \$4}' ++ echo 255.255.255.0</pre>	SI
2	Obtención de cada octeto de la red	<pre>+ octomasc4=0 ++ awk '{ print \$2 }' ++ awk -F 127.0.0.1/8 '{ print \$1 }' ++ grep inet ++ awk -F /24 '{ print \$1 }' ++ awk -F ' ' '{ print \$1 }' ++ ip a ++ sed 1d ++ awk -F . '{ print \$1 }' + octeto1=192 ++ awk -F 127.0.0.1/8 '{ print \$1 }' ++ grep inet ++ awk -F ' ' '{ print \$1 }' ++ ip a ++ sed 1d ++ awk -F . '{ print \$2 }' ++ awk '{ print \$2 }' ++ awk -F /24 '{ print \$1 }' + octeto2=168 ++ awk -F 127.0.0.1/8 '{ print \$1 }' ++ awk '{ print \$2 }' ++ awk -F /24 '{ print \$1 }' ++ grep inet ++ awk -F ' ' '{ print \$1 }' ++ awk -F . '{ print \$3 }' ++ ip a ++ sed 1d + octeto3=0 ++ awk -F 127.0.0.1/8 '{ print \$1 }' ++ awk '{ print \$2 }'</pre>	SI

		<pre> ++ awk -F /24 '{ print \$1 }' ++ grep inet ++ awk -F ' ' '{ print \$1 }' ++ sed 1d ++ ip a ++ awk -F . '{ print \$4 }' + octeto4=115 </pre>	
3	Verificación de la red a escanear	<pre> + expo=8 + hostnum=256 + octetored=0 + inicio=1 + fin=255 + echo 'Red a escanear:' 192.168.0.0 ++ echo 254 + echo 'N. hosts: ' 254 </pre>	SI
4	Conectividad para cada host	<pre> + rango=1 + [[1 -le 255]] + IP=192.168.0.1 + ping 192.168.0.1 -w 3 -c 1 </pre>	SI
5	Estado del host	<pre> + [[1 -eq 1]] + contar=5 + [[5 -eq 10]] + echo '192.168.0.7 pasivo' </pre>	SI
6	Detección del sistema operativo	<pre> + [[" -eq 1]] ++ sed s/Microsoft// ++ sed s/Running:// ++ grep Running: ++ awk '{ print \$1 }' ++ nmap -O 192.168.0.1 </pre>	SI
7	Registro de equipo	<pre> + SOCloud=Wind + [[-z Wind]] + cd /etc/nagios3/conf.d/ ++ find Wind_192.168.0.1.cfg + existe=Wind_192.168.0.1.cfg + echo 192.168.0.1 activo + [[! -z Wind_192.168.0.1.cfg]] + echo 'Equipo ya registrado' </pre>	SI
8	Creación de archivo	<pre> + echo 192.168.0.1 activo 192.168.0.1 activo + [[! -z "]] + /etc/nagios3/conf.d/plantilla 192.168.0.1 Wind + echo " </pre>	SI

Nota. Descripción de resultados obtenido de la ejecución generador de host NAGIOS
Elaborado por: Diego Poveda & Alexis Balarezo

- **Tiempos**

Las pruebas de tiempo de ejecución están implementadas para verificar el comportamiento del Gestor de host NAIGIOS dependiendo el tamaño de la red, consiste en verificar los tiempos tanto en el escaneo de red como en la creación de los archivos de configuración para cada host.

Para la mencionada prueba se ha creado un script de obtención de tiempos de ejecución para el gestor “autodetection.sh”.

Código fuente:

```
tini=$(date +%s)
seg=1000
/etc/ossim/server/autodetection.sh
tfin=$(date +%s)
ttotal=$(( $tfin - $tini ))
segdec=$(echo "$ttotal/$seg" | bc -l | cut -c 1-5)
echo "Tiempo de ejecución: $segdec segundos"
```

- **Análisis**

El Gestor de host NAGOS está dirigido a los administradores de red, que necesitan mejorar los tiempo de repuesta en el monitoreo y manejo de información de la red, por este motivo se ha realizado pruebas de las configuraciones manuales las cuales se asemejan a la realidad mediante la configuración de 3 equipos.

Tabla 22. *Promedio de configuración*

Equipo IP	T. Manual(segundos)	T. Gestor(segundos)
192.168.0.118	10	1.3
192.168.0.119	15	1.0
192.168.0.120	20	1.4
Promedio	15	1.23

Nota. Descripción de los tiempos de promedios de configuración
Elaborado por: Diego Poveda & Alexis Balarezo

Se puede apreciar que el tiempo promedio para el ingreso de un host a la consola de NAGIOS mediante la creación y configuración por el administrador es de 15 segundos y mediante la ejecución del gestor el tiempo es de 1.23 segundos.

Con la obtención de los tiempos promedio se puede concluir que para configurar 1 host mediante la ejecución del Gestor de host NAGIOS es un 91.8% menos que la configuración manual.

- **Gráfica**

En la siguiente ilustración se muestra los resultados previamente obtenidos en forma gráfica, en el que se puede apreciar el promedio de los tiempos de respuesta en la generación de información del Gestor de host NAGIOS y una visualización del tiempo dependiendo del tramo de red en este caso será de 10 a 100 host, el tiempo de configuración del administrador y del gestor será azul y celeste respectivamente.

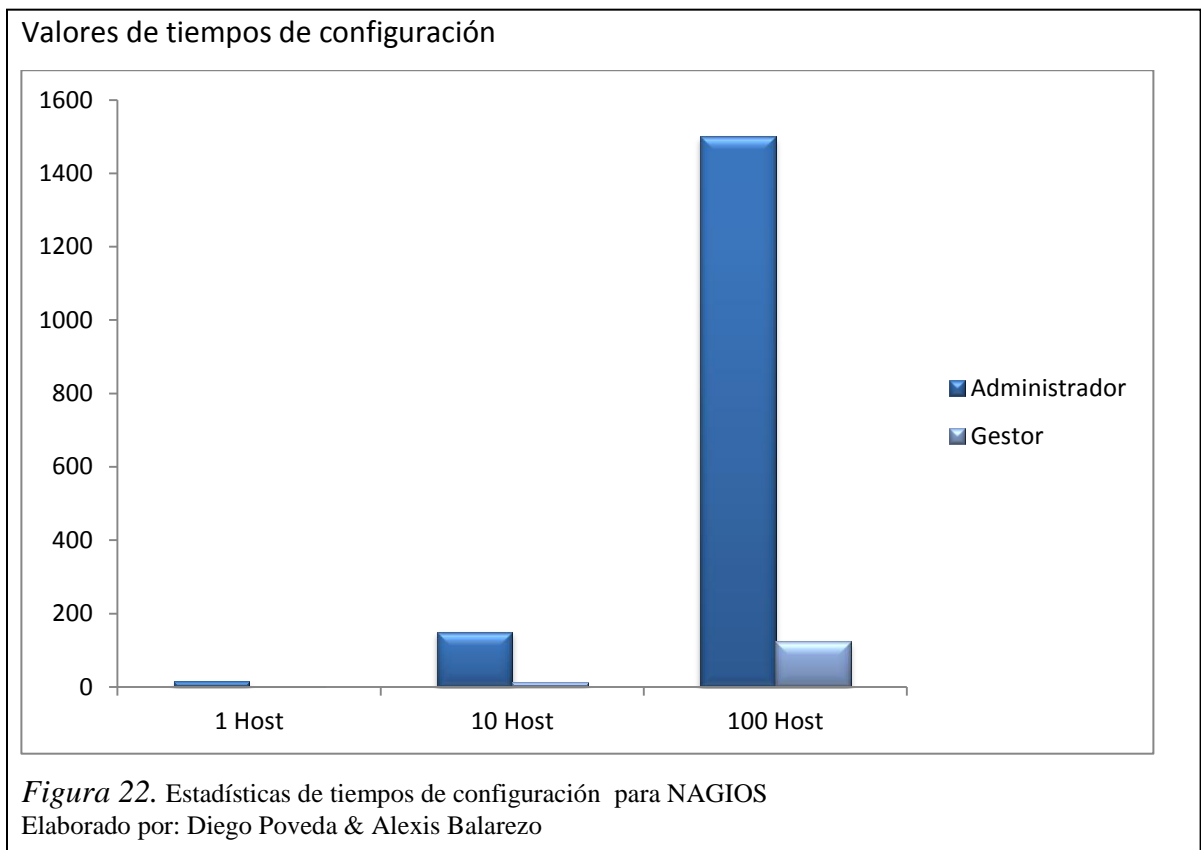


Tabla 23. *Resultados obtenidos*

Configuración	1 Host(segundos)	10 Host(segundos)	100 Hots(segundos)
Administrador	15	150	1500
Gestor	1.23	12.3	123

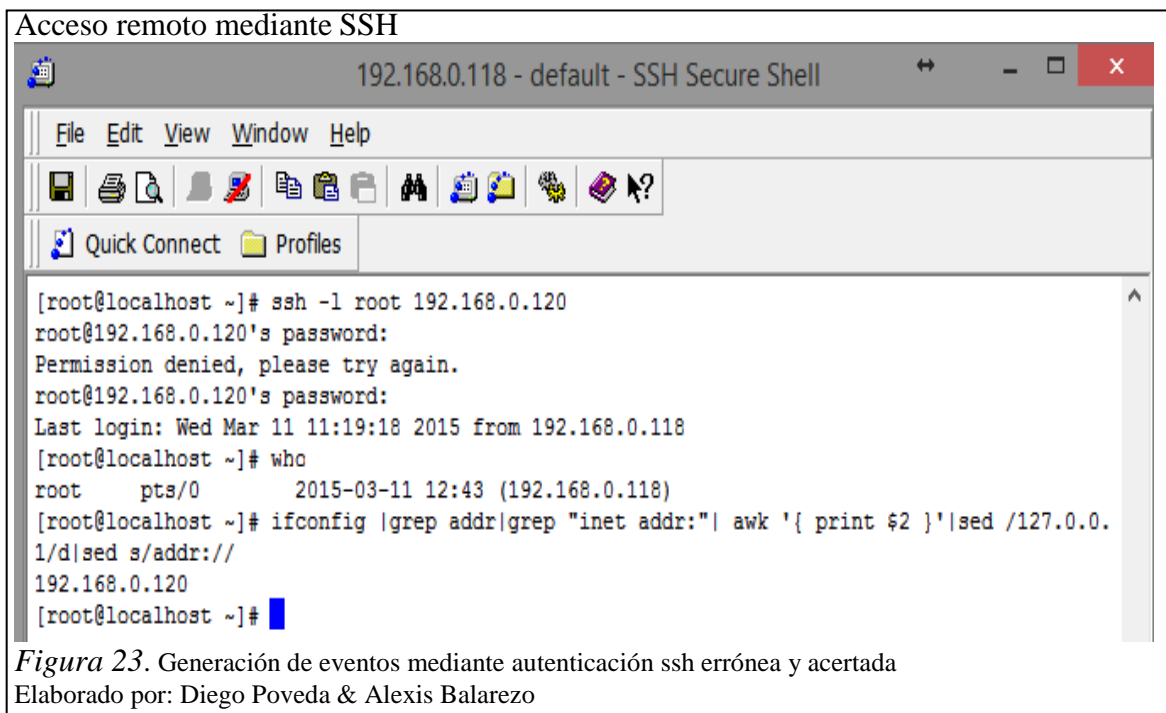
Nota. Descripción de resultados obtenidos con la configuración manual y por medio del gestor
Elaborado por: Diego Poveda & Alexis Balarezo

4.3 Pruebas funcionales OSSEC

Las pruebas funcionales permiten y tienen como objetivo principal la visualización de los resultados obtenidos al implementar los cambios en el código fuente y la optimización de los procesos de la herramienta, mediante estas evaluaciones se puede identificar inconsistencias y las soluciones.

- **Carga**

Estas pruebas fueron realizadas con el objetivo de verificar la optimización del tiempo de respuesta de los eventos generados por la herramienta OSSEC. El proceso consiste en originar eventos en los equipos mediante conexión SSH de manera acertada y desacertada, comparando tiempos de respuesta con y sin la implementación del cambio.



- **Análisis**

La optimización de los tiempos de respuesta de las notificaciones de OSSEC está dirigida a los administradores de seguridades de red para prevenir ataques con mayor rapidez, por tal razón se ha tomado tiempos de respuesta pre-implementación y post-implementación de cambios en las configuraciones y redireccionamiento de rutas manejadas por OSSEC.

Tabla 24. *Medición de tiempos de respuesta generación-visualización eventos*

Generador evento	Pre-implementación		Post-implementación		Mejora tiempo
	Tiempo ingreso	Tiempo salida	Tiempo ingreso	Tiempo salida	
Autenticación correcta	01:38:06	1:38:10	11:19:19	11:19:19	SI
	02:00:39	02:00:43	02:07:51	02:07:55	NO
	02:10:16	02:10:21	02:15:33	02:15:34	SI
Autenticación errónea	11:07:54	11:07:56	11:19:03	11:19:03	SI
	02:00:54	02:00:56	02:09:04	02:09:05	SI
	02:23:19	02:23:21	02:27:00	02:27:00	SI

Nota. Descripción de tiempos resultantes pre y post implementación del cambio
Elaborado por: Diego Poveda & Alexis Balarezo

Como se puede apreciar los tiempos de respuesta mejoran en un 83% aplicando el redireccionamiento y reconfiguración de los archivos al realizar pruebas comparativas tanto en los ingresos regulares mediante SSH con autenticación acertada y errónea.

Considerando los porcentajes de mejora en cuanto a ingresos permitidos es decir con una autenticación autorizada observamos que dos de tres son positivas lo cual certificaría progreso en la herramienta teniendo en cuenta que no se considera como una alerta de alta importancia cuando hay una autenticación satisfactoria. Al analizar las mejoras en el caso de una autenticación que presenta inconvenientes como el password o usuario erróneo observamos una mejora del 100% teniendo como resultados positivos tres de tres en cuanto al tiempo de respuesta, siendo esto un avance para la herramienta ya que al presentarse este tipo de evento hay una probabilidad más elevada de que se trate de un ataque.

Tabla 25. *Promedio comparativo de tiempos pre-post implementación*

Generador evento	Pre-implementación	Post-implementación	Diferencia Tiempo(s)
	Promedio(s)	Promedio(s)	
Autenticación correcta	4.33	1.67	2.66
Autenticación errónea	2	0.33	1.67

Nota. Descripción de tiempos diferencia resultantes pre y post implementación del cambio
Elaborado por: Diego Poveda & Alexis Balarezo

- **Gráfica**

Al analizar la Tabla 25 del promedio comparativo podemos observar que presenta un tiempo significativo de diferencia. Proyectando los resultados de acuerdo a número de host que generen eventos de este tipo simultáneamente se optimiza considerablemente el control de posibles ataques en un tiempo reducido como lo muestra la Tabla 26.

Tabla 26. *Optimización de tiempos de respuesta por host*

Generador evento	Pre-implementación			Post-implementación		
	1 HOST	10 HOST	100 HOST	1 HOST	10 HOST	100 HOST
Autenticación correcta	4.33	43.3	433	1.67	16.7	167
Autenticación errónea	2	20	200	0.33	3.3	33

Nota. Descripción de tiempos resultantes pre y post implementación del cambio con escalamiento de host
Elaborado por: Diego Poveda & Alexis Balarezo

Como se puede apreciar en la Tabla 26 tomando el tiempo promedio de las pruebas realizadas se reduce ampliamente el periodo de respuesta de acuerdo al número de host que generen el evento simultáneamente.

Valores tiempo visualización de eventos autenticación correcta

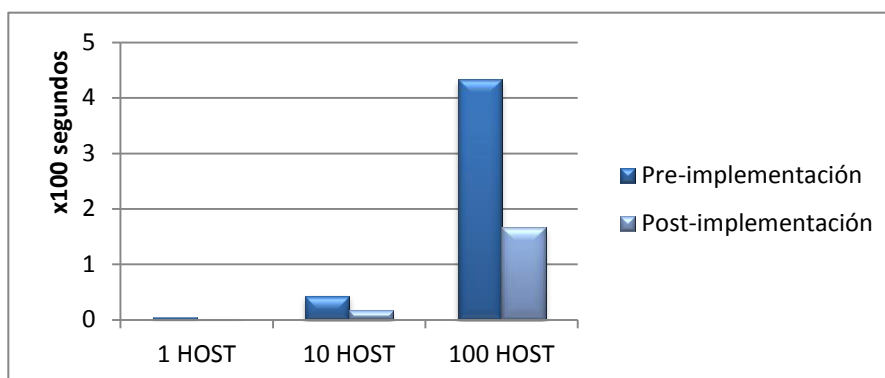


Figura 24. Tiempo promedio de visualización de eventos autenticación correcto
Elaborado por: Diego Poveda & Alexis Balarezo

En la Figura 24, se puede visualizar el promedio de eventos realizados en la autenticación en forma correcta antes de la implantación de los cambios y posteriormente a los cambios realizados, las pruebas se realizaron con 1 host, 10 host y 100 host.

Valores tiempo visualización de eventos autenticación errónea

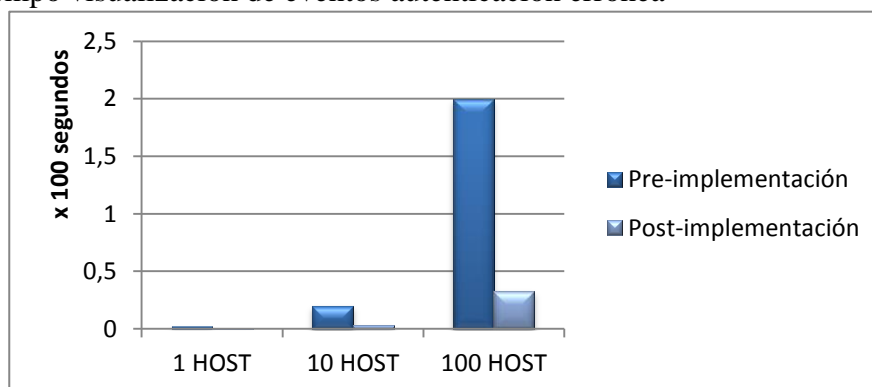


Figura 25. Tiempo promedio de visualización de eventos autenticación erróneo
Elaborado por: Diego Poveda & Alexis Balarezo

En la Figura 25, se puede visualizar el promedio de eventos realizados en la autenticación en forma errónea antes de la implantación de los cambios y posteriormente a los cambios realizados, las pruebas se realizaron con 1 host, 10 host y 100 host.

CONCLUSIONES

- La principal ventaja que se tiene con la Cloud Computing es su alta adaptabilidad, ya que esto permite que se tengan las máquinas virtuales actualizadas sin intervención del usuario, esto es muy importante ya que si el usuario realiza la actualización por su propia cuenta esta podría ser obsoleta y se tendría que crear nuevamente, siempre teniendo en cuenta el valor económico que implicaría por el proceso de una nueva instalación.
- Basándose en la metodología PPIDOO se consiguió diseñar e implementar una estructura de red la cual contiene un sistema Cloud Computing de tipo privado con una fuente de almacenamiento RAID 5 que permite tener una infraestructura de alta disponibilidad, la misma que esta monitoreada con el sistema OSSIM el cual está ejecutándose en el servidor central, con las mejoras realizadas al sistema OSSIM podemos concluir que es un proyecto de gran utilidad ya que todos los sistemas del laboratorio son de código abierto lo que implica que no existe costo por adquisición e implantación.
- OSSIM es una herramienta de monitoreo y detección que permite verificar las amenazas en tiempo real ya que está basada en la tecnología SIEM. A pesar de que esta herramienta trabaja de forma inteligente ya que es capaz de correlacionar eventos en busca de patrones que identifiquen un ataque exige varias horas de configuración para lograr la ejecución acorde a las necesidades y llegar a un funcionamiento óptimo.
- La herramienta OSSIM permite el análisis de los eventos que son recolectados en los archivos de logs que están en la red esto ayuda a descubrir posibles ataques, todo esto se logra mediante las herramientas de monitoreo y detección que se encuentran integradas en OSSIM, al estar integradas estas herramientas en una sola plataforma permiten realizar un análisis para realizar posibles integraciones para obtener una mejor administración.

- El sistema OSSIM se caracteriza por trabajar en forma inteligente ya que esta herramienta es capaz de correlacionar los eventos que se generan en la red para localizar algún patrón que identifique a un ataque, una vez detectado el patrón se configura en OSSIM las políticas para que se lance una alarma que informe el suceso, toda esta información de los suceso hace que se pueda prevenir incidentes conociendo los datos de los eventos ya registrados con anterioridad, para obtener mejores resultados es importante configurara correctamente las políticas.
- El manejo de NMAP y NAGIOS en una sola consola mediante OSSIM permite integrar sus datos para obtener beneficios mediante la reducción de los tiempos de configuración y ejecución por parte del administrador, estas herramientas al obtener y recolectar parámetros similares permiten que se obtenga información esencial la cual se puede gestionar por NMAP para configurar y crear archivos en NAGIOS en forma automática que permiten desplegar los equipos a monitorear en el hipervisor en un tiempo reducido.

RECOMENDACIONES

- Se recomienda que el sistema de Cloud Computing sea instalado en una equipo que posea como mínimo 8 GB de RAM y que permite el aumento de memoria dependiendo el número de equipos que serán instalados para ofrecer el servicio, se debe considera que para obtener un mejor desempeño del sistema se debe instalar y configurar en un sistema de 64bits. El almacenamiento de la Cloud Computing es recomendable diseñarlo con un sistema RAID basado en software ya que implicaría un costo solamente en la adquisición de los dispositivos de almacenamiento.
- Es de suma importancia que todas la políticas que se generen en OSSIM estén configuradas correctamente y siempre actualizadas dependiendo de las reglas o políticas de seguridad de la empresa en la que se tenga levantado el servicios de OSSIM. A pesar que esta herramienta tienen una serie de políticas preconfiguradas, es necesario que el administrador de la seguridad configure las policías acorde al entorno que presenta la empresa, es recomendable que toda regla o política sea implantada por personal que tenga un alto conocimiento de la arquitectura de seguridad que se encuentre en la entidad.
- Para tener un mejor rendimiento de las herramientas de monitoreo se recomienda el análisis funcional el cual permita obtener una mejora en la administración de la información y una automatización de los procesos, dependiendo el análisis y la necesidad se podría llegar a mejor las capacidades y los tiempos de respuesta de los sistemas de código abierto y con esto reducir costos significativos para la empresa.
- Para el mejoramiento, soporte y mantenimiento de las nuevas funcionalidad que sean implementadas a OSSIM el código debe ser distribuido a la comunidad de Open Source para que sea certificado y se lo pueda generar en una versión estable. Esto es de suma importancia ya que la colaboración en la actualización de los servicios que ofrece OSSIM permite que cada vez se eviten más ataques a los sistemas informáticos.

LISTA DE REFERENCIAS

- Departamento de Postgrados de la Universidad del Valle de México. (2009). *Manual de Normas y Politicas de Seguridad Informatica*. Obtenido de <http://www.scribd.com/doc/211891283/ISO-27000-Manual-de-Normas-y-Policas-de-Seguridad-Informatica#scribd>
- Dorat, M., & Moran, J. (15 de Enero de 2015). *Evaluación de NAGIOS para Linux*. Obtenido de http://nagios.sourceforge.net/download/contrib/documentation/misc/Nagios_spanish.pdf
- Estación Informática. (11 de 12 de 2013). *OSSIM SISTEMA DE GESTIÓN DE LA INFORMACIÓN OPENSOURCE*. Obtenido de <http://www.estacion-informatica.com/2013/12/ossim-sistema-de-gestion-de-la.html>
- Larador, R. (10 de Enero de 2015). *Programación avanzada en SHELL*. Obtenido de http://www.forpas.us.es/documentacion/programacion_avanzada_en_shell.pdf
- Martinez, L. (3 de 5 de 2013). *Mi análisis de alienvault/OSSIM 4.2.1*. Obtenido de <http://securitybydefault.com/2013/05/mi-analisis-de-alienvaultossim-421.html>
- Mike, G. (22 de Diciembre de 2014). *Programación en BASH*. Obtenido de <http://es.tldp.org/COMO-INSFLUG/es/pdf/Bash-Prog-Intro-COMO.pdf>
- Miller, D., Harrys, S., Harper, A., & VanDyke, S. (2010). *Security Information and Event Management (SIEM) Implementation*. Florida: Mc GranHill.
- Párrigas, A. (22 de Enero de 2015). *OSSIM, una plataforma clave para la seguridad en profundidad*. Obtenido de <http://www.angelalonso.es/doc-presentaciones/ossim-hakin9.pdf>
- Security Standards Council. (Noviembre de 2013). *Requisitos y procedimientos de evaluación de Seguridad Versión 3.0*. Obtenido de https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3.pdf

GLOSARIO DE TÉRMINOS

Open Source: Expresión con la que se conoce al software distribuido y desarrollado libremente.

OSSIM: Open Source Security Information Management por sus siglas es una colección de herramientas bajo la licencia GPL, diseñadas para ayudar a los administradores de red en la seguridad de las computadoras, detección de intrusos y prevención.

SEM: Gestión de Eventos, proporciona monitoreo en tiempo real y gestión de eventos de TI de apoyo a las operaciones de seguridad.

SIM: Gestión de la Seguridad de la Información, permite tener un historia de los sucesos.

Monitor: Realiza una monitorización de la red ayudando al administrador de seguridad a reconocer si un evento está presentando alguna actividad anómala.

Sensor: Recoge los logs de los diferentes dispositivos electrónicos y aplicaciones de seguridad.

AlienVault: Es un sistema unificado de gestión de seguridad, el cual integra una serie de herramientas para la seguridad informática.

Cloud Computing: La computación en la nube, concepto conocido también bajo los términos servicios es un paradigma que permite ofrecer servicios de computación a través de Internet.

XCP, XenServer: Plataforma de virtualización de código abierto líder en el sector empresarial para administrar las infraestructuras virtuales.

XenCenter: Es el administrador web de XenServer.

RAID: RedundantArray of Independent Disks), esta tecnología fue diseñada para crear arreglos de discos duros.

Phishing: Término informático que denomina un tipo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta.

Hipervisores: Plataforma que permite aplicar diversas técnicas de control de virtualización para utilizar, al mismo tiempo, diferentes sistemas operativos en una misma computadora.

Proxy: Puede ser una red informática, un servidor que sirve de intermediario en las peticiones de recurso.

DNS: Abreviatura para Sistema de nombre de dominios, que permite asignar nombres a equipos y servicios de red.

NAS: Network-Attached Storage, es el nombre dado a una tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento.

Kernel: Software que constituye una parte fundamental del sistema operativo.

Virtualización: Es la creación a través de software de una versión virtual de algún recurso tecnológico.

root: Usuario genérico en Linux que tiene acceso administrativo al sistema.

ISO: Archivo donde se almacena una copia o imagen exacta de un sistema de ficheros, normalmente un disco óptico.

Data Center: Centro de proceso de datos es una ubicación que concentra todos los recursos físicos para el procesamiento de la información de una empresa u organización.

VM: es una máquina virtual.

Parser: Conjunto de procesos que maneja OSSIM.

Plugins: Archivo de configuración de servicios que permiten la obtención de información mediante las herramientas que integra OSSIM.

HTTP: Protocolo de transferencia de hipertextos, que se utiliza en algunas direcciones de internet.

SMTP: Protocolo de la capa de aplicación. Protocolo de red basado en texto, utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos.

ICMP: Protocolo de Mensajes de Control de Internet o ICMP es el sub protocolo de control y notificación de errores del Protocolo de Internet.

POP3: Es un protocolo de red que se utiliza en clientes locales de correo electrónico para obtener los mensajes de correo almacenados en un servidor remoto.

SSH: Sirve para acceder a máquinas remotas a través de una red.

ANEXOS

Anexo 1. Configuración RAID 5

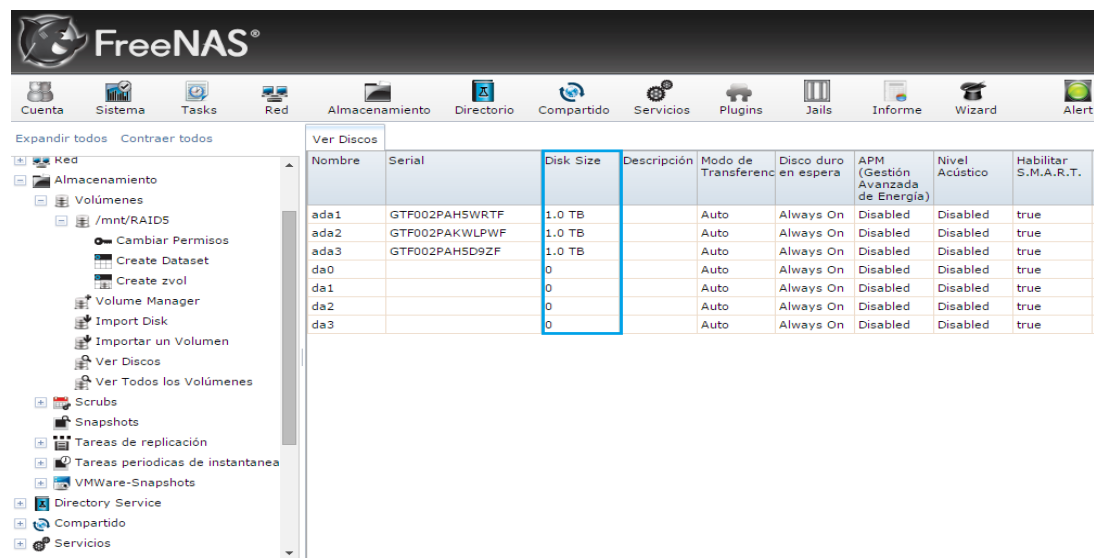
- **Pantallas configuración FreeNAS.**

La configuración del servidor NAS se la realizó directamente en la máquina que posee las siguientes características:

- Procesador Core2Duo 2.66 GHz
- Memoria RAM 4 Gb
- 3 Discos Duros de 1TB
- 1 Disco Duro de 500GB

La pantalla de identificación y reconocimiento de los disco duros permite visualizar los volúmenes de cada dispositivos para verificar su tamaño y descripción, se debe tener en cuenta que solamente se puede generar un RAID 5 si la capacidad de almacenamiento de los dispositivos es igual.

Verificación del tamaño de los discos duros



Nombre	Serial	Disk Size	Descripción	Modo de Transferencia	Disco duro en espera	APM (Gestión Avanzada de Energía)	Nivel Acústico	Habilitar S.M.A.R.T.
ada1	GTF002PAH5WRTF	1.0 TB		Auto	Always On	Disabled	Disabled	true
ada2	GTF002PAKWLPWF	1.0 TB		Auto	Always On	Disabled	Disabled	true
ada3	GTF002PAH5D9ZF	1.0 TB		Auto	Always On	Disabled	Disabled	true
da0		0		Auto	Always On	Disabled	Disabled	true
da1		0		Auto	Always On	Disabled	Disabled	true
da2		0		Auto	Always On	Disabled	Disabled	true
da3		0		Auto	Always On	Disabled	Disabled	true

Figura. Descripción de los dispositivos físicos y su capacidad

Elaborado por: Diego Poveda & Alexis Balarezo

La pantalla de configuración de FreeNAS permite la creación del dispositivo lógico, el cual, será el resultado de la unión de los dispositivos físicos, con una configuración adecuada se puede crear diferentes niveles de RAID.

Elección de los dispositivos que formaran el RAID5

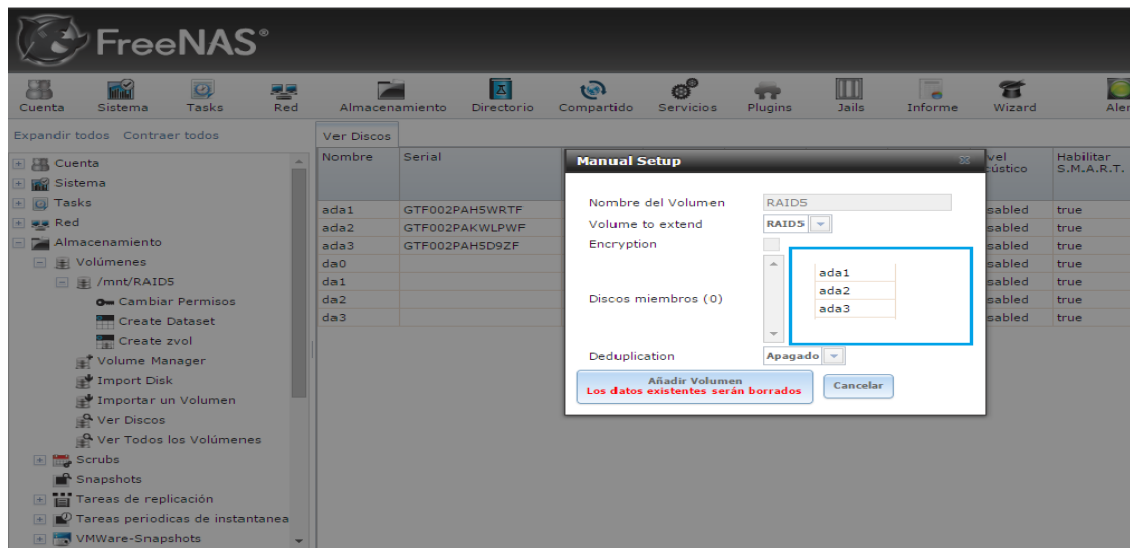


Figura. Creación del volumen lógico.

Elaborado por: Diego Poveda & Alexis Balarezo

La pantalla para compartir el disco lógico muestra la ubicación en la cual se almacenará los datos que recibirá y tendrá la Cloud Computing, esta ruta se puede cambiar dependiendo la necesidad del administrador, es recomendable habilitar todos los permisos para no presentar problemas al momento de ingresar la dirección y crear al disco lógico de la nube.

Ruta del dispositivo lógico para el almacenamiento

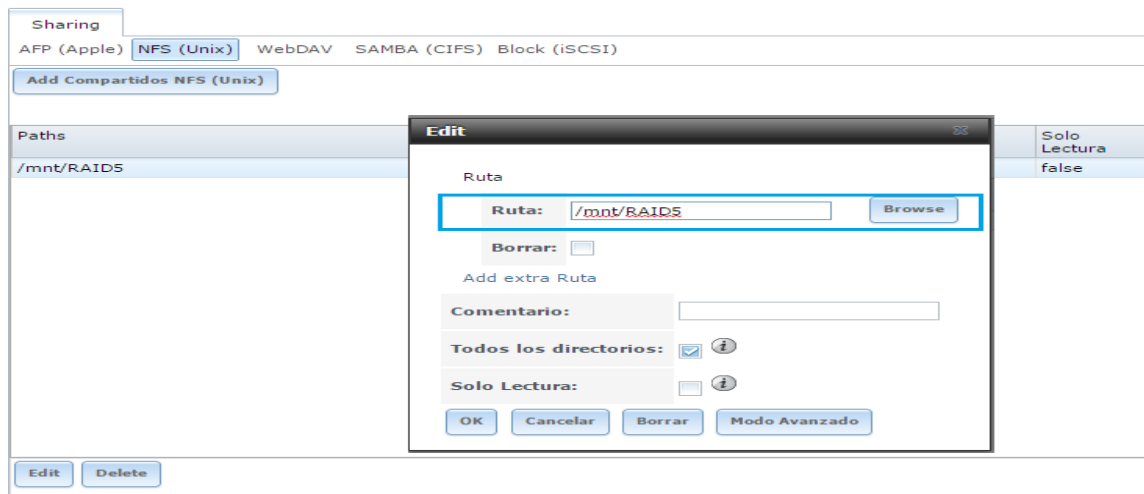


Figura. Descripción de los dispositivos físicos y su capacidad

Elaborado por: Diego Poveda & Alexis Balarezo

- **Pantallas configuración XenServer**

- Procesador Dual Core 2.9 GHz
- Memoria RAM 8 Gb
- 1 Discos Duros 160 GB

The screenshot displays the XenServer 6.5 configuration console. The title bar reads 'XenServer 6.5 17:40:55 xenserver-ossim'. The main menu on the left lists various configuration options, with 'Network and Management Interface' selected and highlighted. The right pane shows the configuration for this interface, including the current management network connection settings (hostname, NTP) and the current management interface details (device, MAC address, DHCP/Static IP, IP address, netmask, gateway, hostname, and NTP status). The console is running on a terminal with a red background.

Configuration Item	Value
Current Management Interface	
Device	eth1
MAC Address	00:08:54:34:40:9a
DHCP/Static IP	Static
IP address	192.168.0.105
Netmask	255.255.255.0
Gateway	192.168.0.1
Hostname	xenserver-ossim
NTP	Enabled

81

Conexión XenServer mediante XenCenter

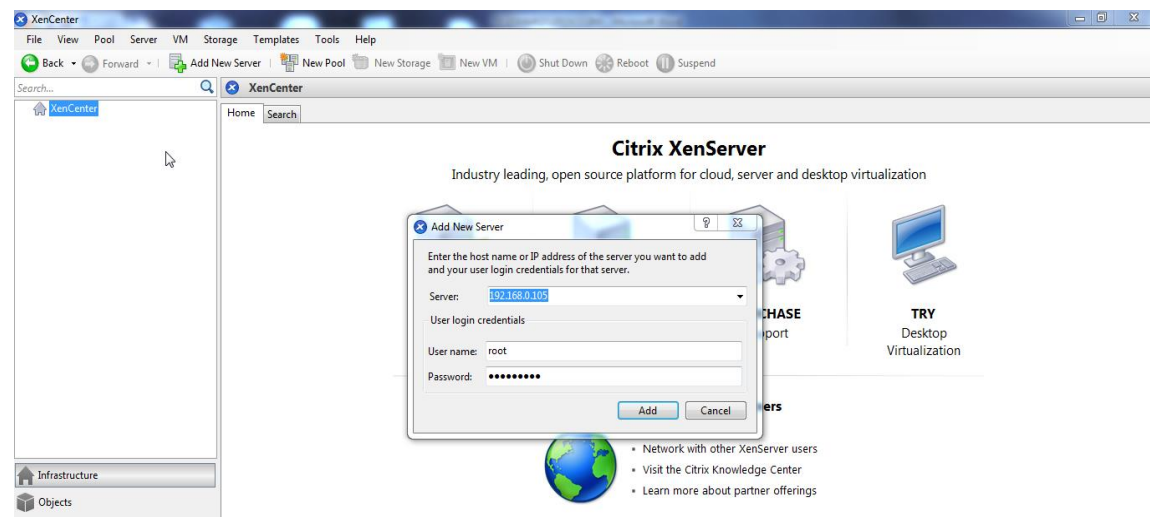


Figura. Menú de configuración XenServer
Elaborado por: Diego Poveda & Alexis Balarezo

Realizada la conexión al XenServer se procede a configurar el disco de almacenamiento que contendrá a las máquinas virtuales, la cuales, tendrá una alta disponibilidad gracias al ya creado RAID5. Se debe ingresar la dirección del servidor y la ruta en la cual se almacenara la información.

Configuración del depósito de almacenamiento

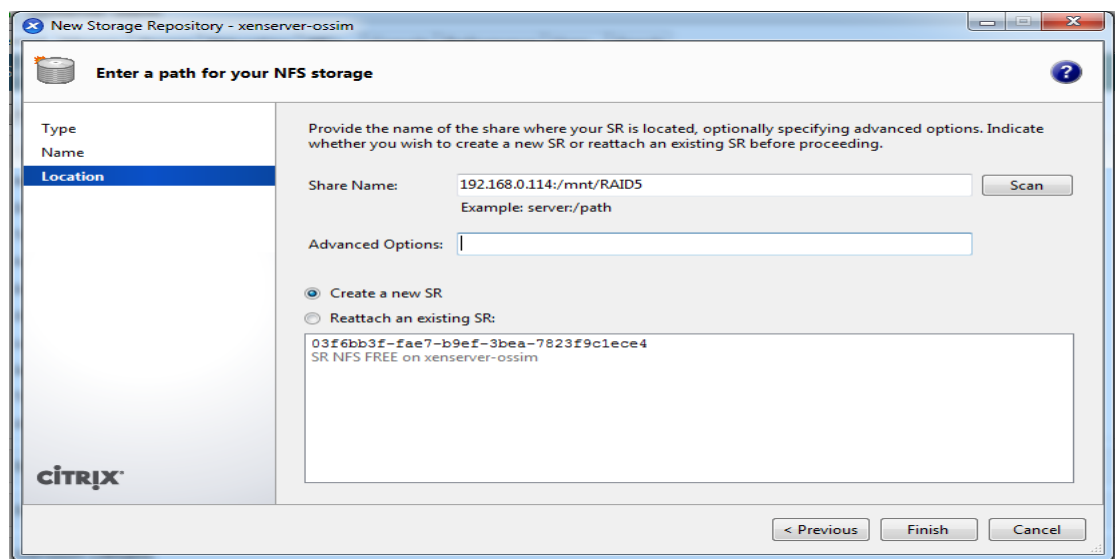


Figura. Conexión al dispositivo lógico
Elaborado por: Diego Poveda & Alexis Balarezo

Reconocimiento de la capacidad de almacenamiento

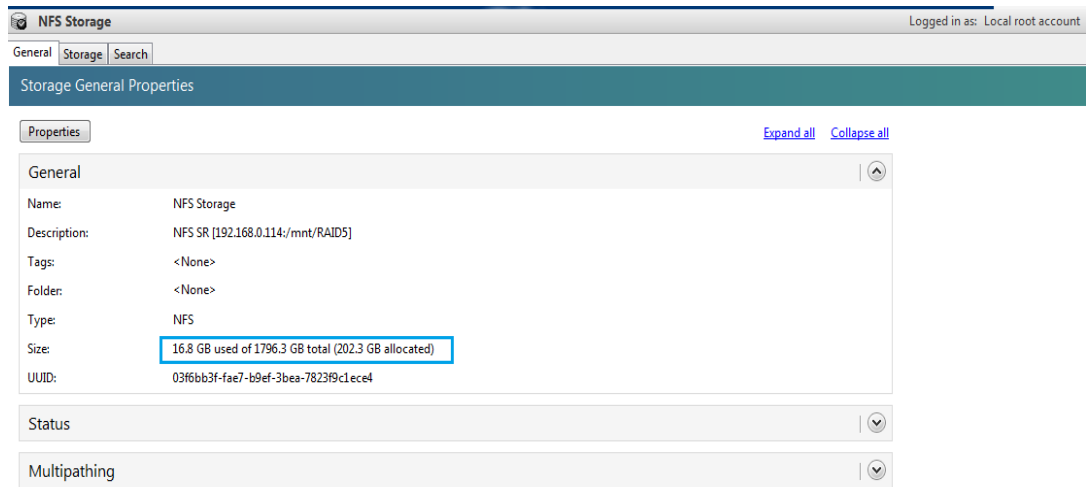


Figura. Dispositivo lógico asignado a la Cloud Computing
Elaborado por: Diego Poveda & Alexis Balarezo

Para la creación de cualquier máquina virtual en la nube se crea un repositorio en el cual se copiarán las imágenes ISO de los dispositivos virtuales a instalar.

Elección de la imagen ISO

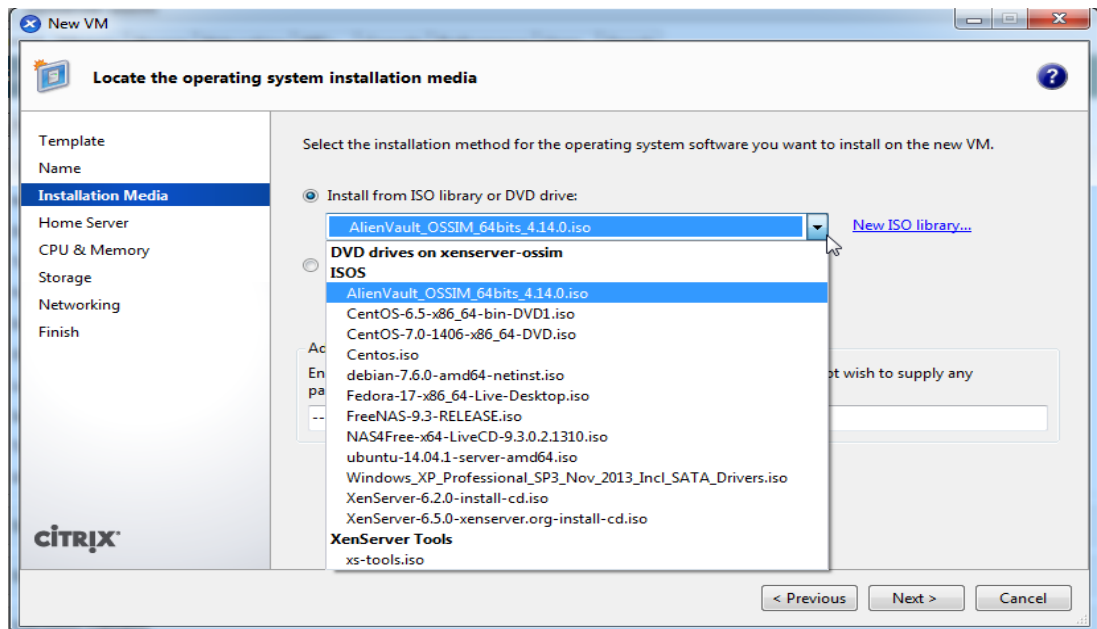


Figura. Conexión al dispositivo lógico
Elaborado por: Diego Poveda & Alexis Balarezo

Para la creación de los nodos se configura un servidor XenServer, el cual, contendrá a los 3 nodos y cada uno será un XenServer.

XenServer principal

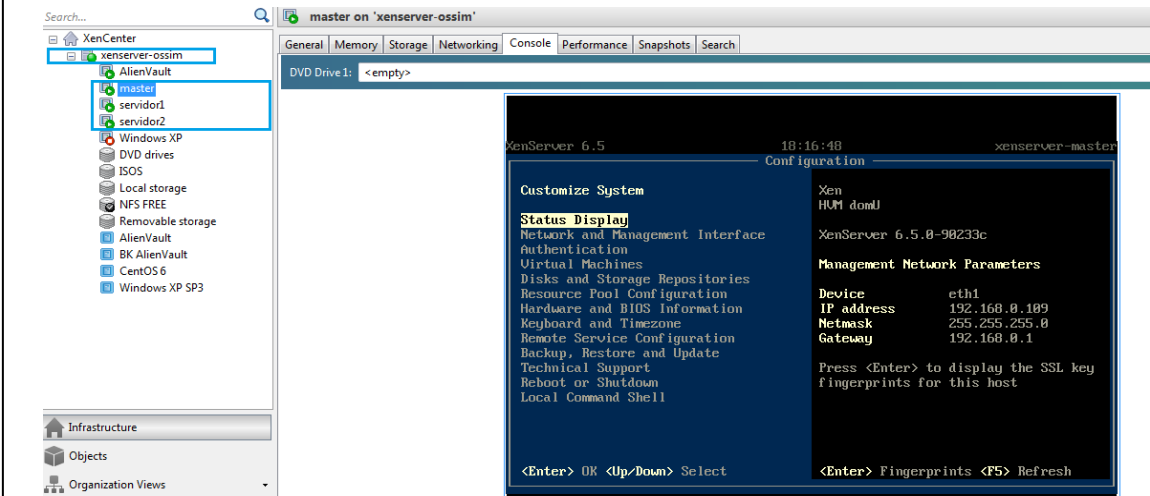


Figura. Laboratorio XenServer , nodo máster, nodo 1 y nodo 2

Elaborado por: Diego Poveda & Alexis Balarezo

Creado los nodos en la nube principal se procede a realizar la conexión a los mismos y continuar con la instalación de los dispositivos virtuales.

Conexión a los nodos

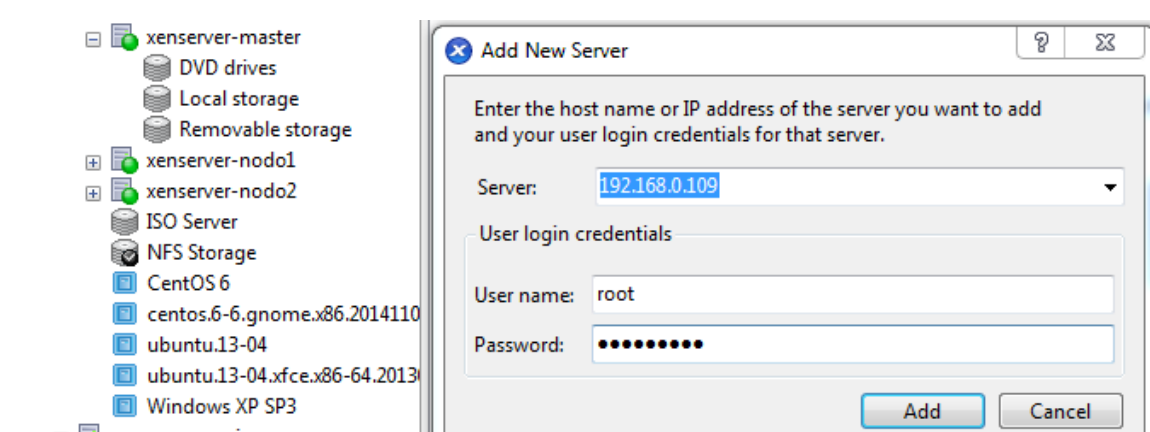


Figura. Conexión a los 3 nodos XenServer

Elaborado por: Diego Poveda & Alexis Balarezo

Realizada la conexión de los nodos se procede a crear las máquinas virtuales que serán los servicios que se ofrecerán al cliente en el presente laboratorio.

Creación de máquinas virtuales clientes

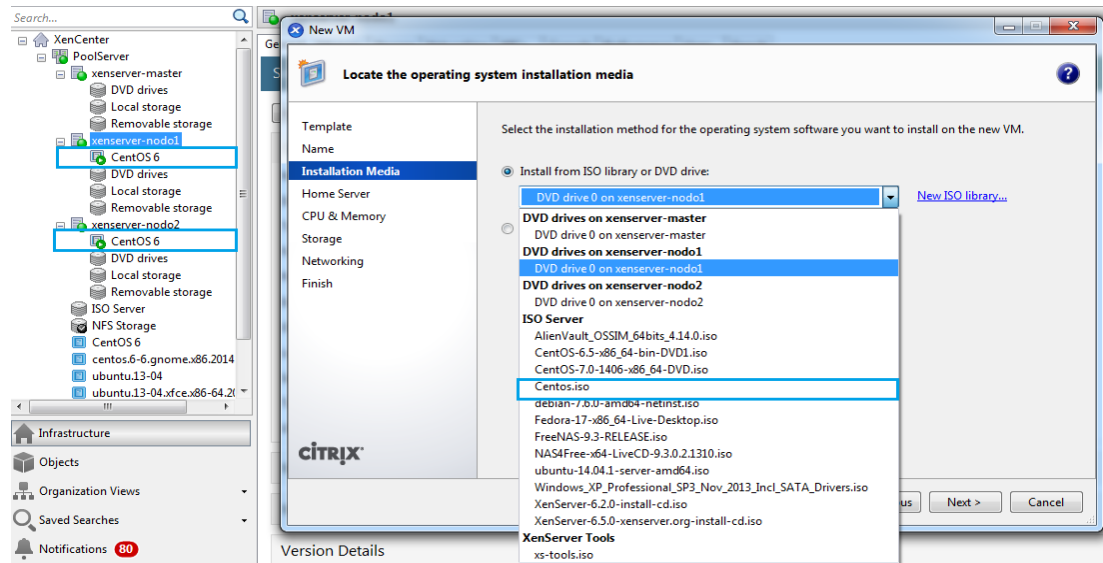


Figura. Creación e instalación de las VM en los nodos secundarios
Elaborado por: Diego Poveda & Alexis Balarez

Una vez creadas las máquinas virtuales y asignadas a cada nodo, se necesita crear un Pool el cual permite integrar los nodos en una sola infraestructura, con el Pool iniciado se configura la alta disponibilidad para que se tenga redundancia en los nodos al presentarse algún fallo.

Pool de nodos

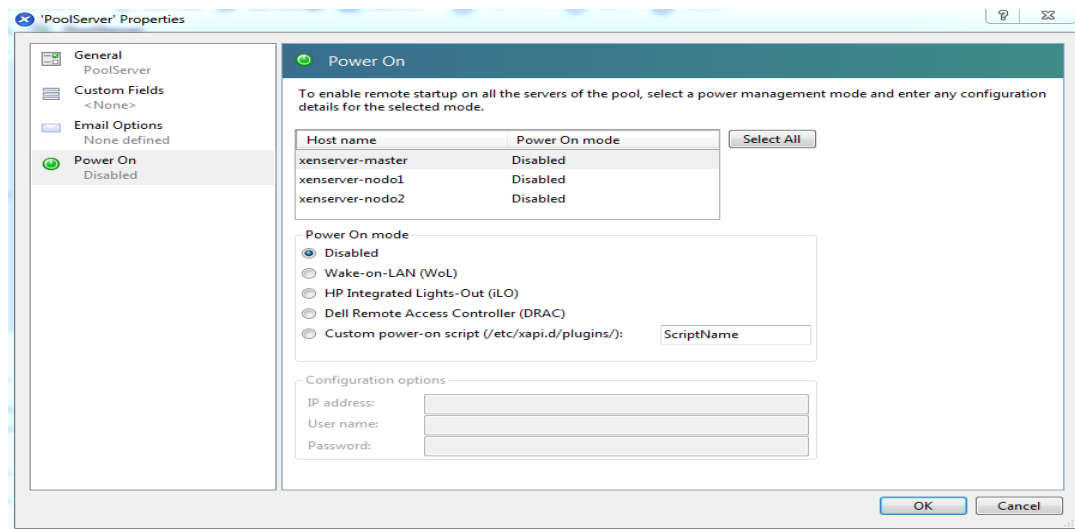


Figura. Creación Pool de nodos
Elaborado por: Diego Poveda & Alexis Balarez

Alta disponibilidad

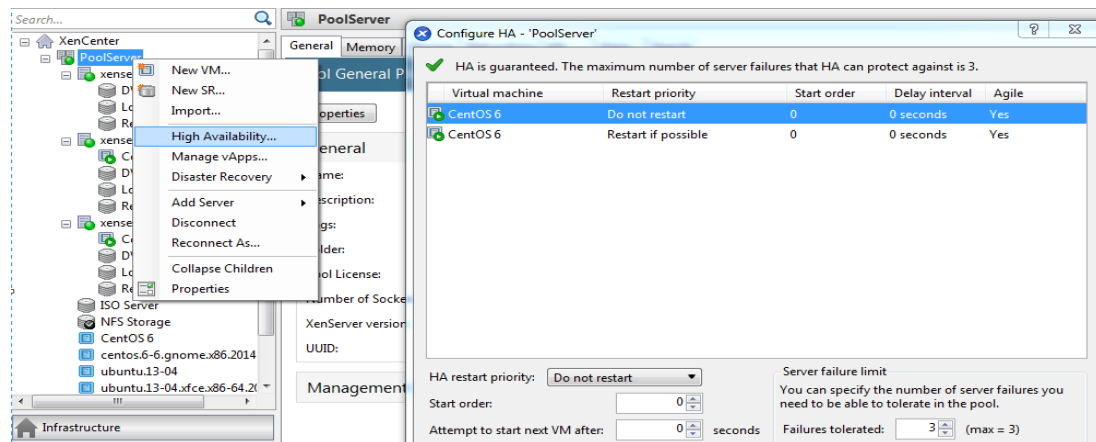


Figura. Habilitación alta disponibilidad en el Pool
Elaborado por: Diego Poveda & Alexis Balarezo

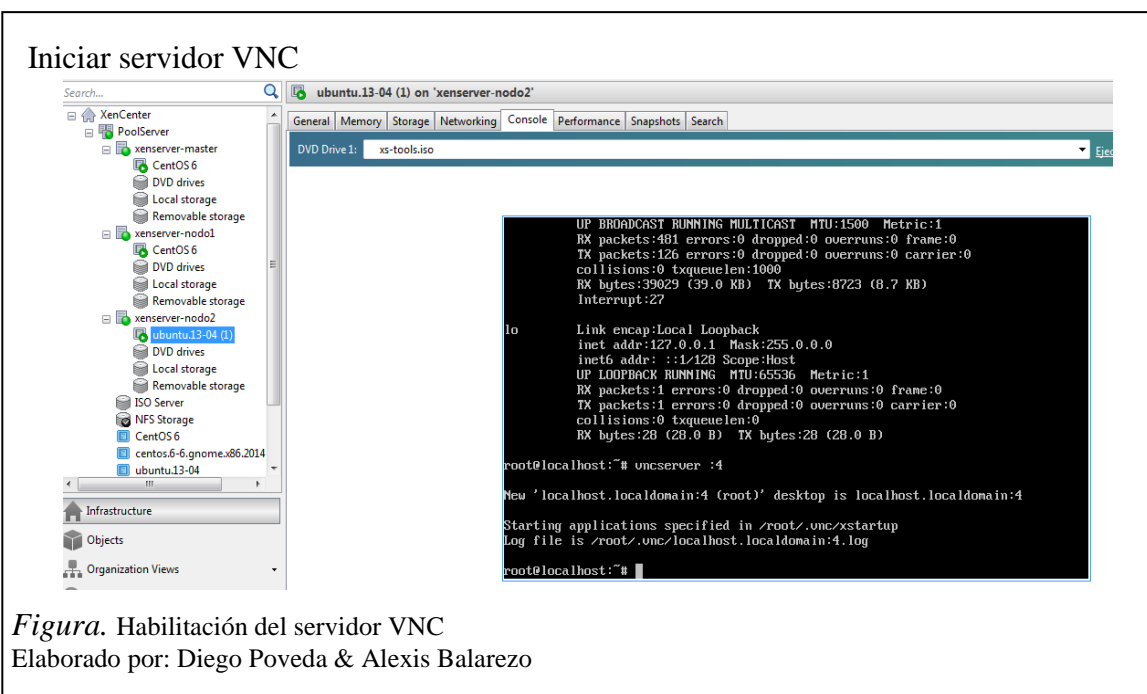
Anexo 3. Accesos máquinas virtuales

- **Pantallas acceso máquinas virtuales.**

Para realizar el acceso a las máquinas virtuales creadas en la nube en este caso los equipos cliente Linux, se configurará el servicio VNC e instalará el cliente VNC en el usuario que solicita el servicio.

Configuración VNC máquina virtual.

```
cd /mnt
mkdir xs-tools
mount /dev/xvdd /mnt/xs-tools
cd /mnt/xs-tools/Linux
ls
bash install.sh
dpkg -i *_i386.deb esto depende de la distribución del sistema
vncserver :4
```



Una vez iniciado el servicio VNC se debe ingresar a la máquina virtual mediante el acceso VNC que se encuentra instalado en el cliente, para este caso se ingresará desde

un equipo con IP: 192.168.0.104 en el cual se encuentra instalado un sistema Windows como anfitrión a la VM de la nube con IP: 192.168.0.130.

Conexión cliente VNC

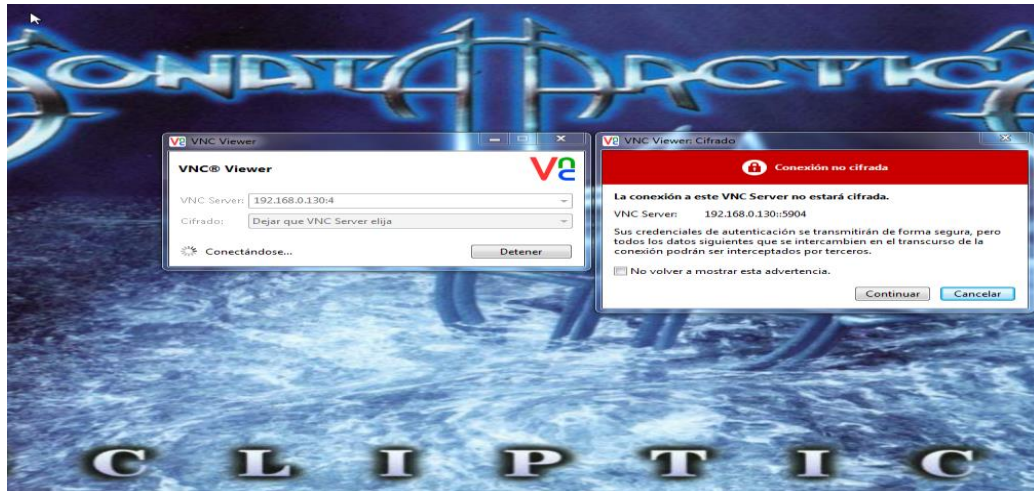


Figura. Habilitación del servidor VNC
Elaborado por: Diego Poveda & Alexis Balarezo

Acceso máquina virtual cliente

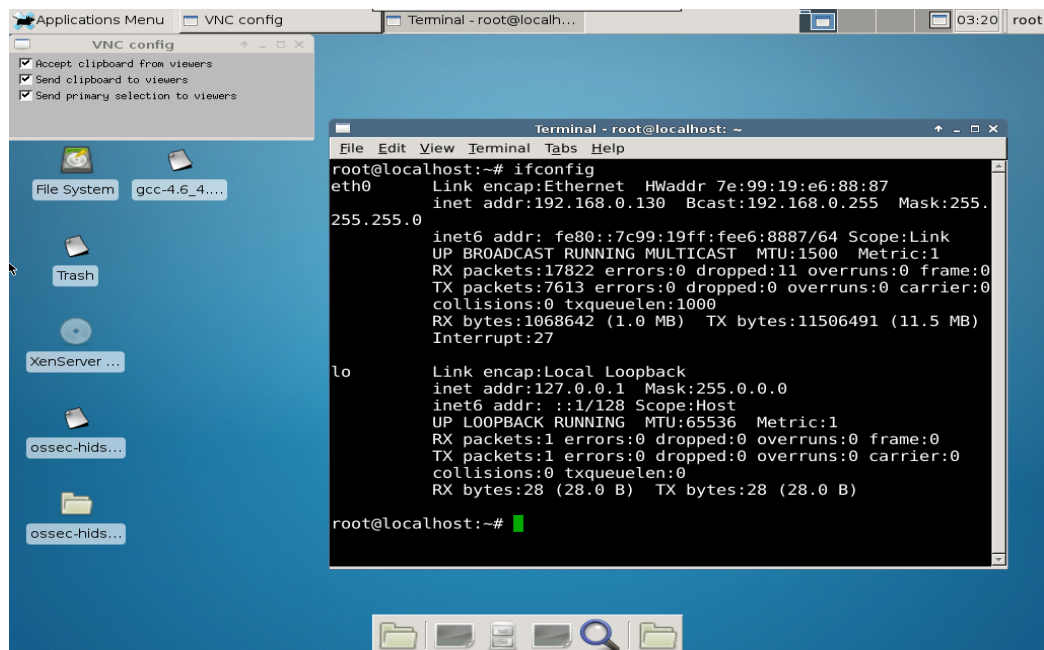


Figura. Conexión al equipo virtual 192.168.0.130
Elaborado por: Diego Poveda & Alexis Balarezo

Anexo 4. Gestor de host NAGIOS

- **Pantallas ejecución del Gestor de host NAGIOS**

A continuación se muestra la ejecución del Gestor de host NAGIOS el cual fue añadido en el archivo rc.local para que se escanee la red y configure de forma automática los archivos de gestión de NAGIOS, al iniciar el sistema OSSIM.

Ejecución Gestor de host NAGIOS

```
Loading, please wait...
Begin: Loading essential drivers ... done.
Begin: Running /scripts/init-premount ... Cannot get device ring settings: Operation not supported
/etc/rc.local: line 8: /sys/block/sda/queue/scheduler: No such file or directory
Red a escanear: 192.168.0.0
N. hosts: 254
find: `Wind_192.168.0.1.cfg': No such file or directory
192.168.0.1 activo
TIEMPO REGISTRO EQUIPO 192.168.0.1: .8000 SEG

192.168.0.59 pasivo
find: `HOST_192.168.0.100.cfg': No such file or directory
192.168.0.100 activo
TIEMPO REGISTRO EQUIPO 192.168.0.100: .5000 SEG

find: `Windows_192.168.0.101.cfg': No such file or directory
192.168.0.101 activo
TIEMPO REGISTRO EQUIPO 192.168.0.101: .3000 SEG

192.168.0.103 pasivo
find: `Windows_192.168.0.104.cfg': No such file or directory
192.168.0.104 activo
TIEMPO REGISTRO EQUIPO 192.168.0.104: .5000 SEG

find: `Linux_192.168.0.105.cfg': No such file or directory
192.168.0.105 activo
TIEMPO REGISTRO EQUIPO 192.168.0.105: .7000 SEG
```

Figura. Ejecución automática del Gestor de host NAGIOS

Elaborado por: Diego Poveda & Alexis Balarezo

El Gestor puede ser ejecutado cada vez que el administrador lo desee, se debe ingresar a la consola de OSSIM en la dirección “/etc/ossim/server” y ejecutarlo, se debe tener en cuenta que el Gestor de host NAGIOS consumirá una cantidad considerable de recursos.

Ejecución manual Gestor de host NAGIOS

```
find: `HOST_192.168.0.111.cfg': No such file or directory
192.168.0.111 activo
TIEMPO REGISTRO EQUIPO 192.168.0.111: 1.501 SEG

192.168.0.113 pasivo
find: `FreeBSD_192.168.0.114.cfg': No such file or directory
192.168.0.114 activo
TIEMPO REGISTRO EQUIPO 192.168.0.114: .9000 SEG

find: `HOST_192.168.0.115.cfg': No such file or directory
192.168.0.115 activo
TIEMPO REGISTRO EQUIPO 192.168.0.115: 1.200 SEG

192.168.0.117 pasivo
find: `Linux_192.168.0.118.cfg': No such file or directory
192.168.0.118 activo
TIEMPO REGISTRO EQUIPO 192.168.0.118: .9000 SEG

192.168.0.119 pasivo
find: `Linux_192.168.0.120.cfg': No such file or directory
192.168.0.120 activo
TIEMPO REGISTRO EQUIPO 192.168.0.120: .8010 SEG

192.168.0.129 pasivo
find: `Linux_192.168.0.130.cfg': No such file or directory
192.168.0.130 activo
TIEMPO REGISTRO EQUIPO 192.168.0.130: .3000 SEG

192.168.0.209 pasivo
Restarting nagios3 monitoring daemon: nagios3Waiting for nagios3 daemon to die...
escaneo completo
alienvault:/etc/ossim/server# ./autodetection.sh
```

Figura. Ejecución manual de Gestor de host NAGIOS

Elaborado por: Diego Poveda & Alexis Balarezo

Ingreso al administrador Web de OSSIM



Figura. Ingreso al sistema OSSIM
Elaborado por: Diego Poveda & Alexis Balarezo

La pantalla para verificar la disponibilidad de los servicios que se encuentran activos en los equipos escaneados y configurados para la visualización en la consola de NAGIOS, permite verificar la información de cada máquina virtual ingresada.

Pantalla de visualización NAGIOS

Host	Service	Status	Last Check	Next Check	Output
Linux_192.168.0.120	Current Load	OK	2015-03-10 23:18:56	0d 0h 19m 36s	1/4 OK - load average: 2.40, 2.13, 1.34
	Current Users	OK	2015-03-10 23:19:40	0d 0h 18m 52s	1/4 USERS OK - 1 users currently logged in
	Disk Space	OK	2015-03-10 23:20:24	0d 0h 18m 8s	1/4 DISK OK
	HTTP	CRITICAL	2015-03-10 23:18:09	0d 0h 17m 24s	4/4 No route to host
	PING	OK	2015-03-10 23:18:10	0d 0h 16m 40s	1/4 PING OK - Packet loss = 0%, RTA = 9.43 ms
	SSH	OK	2015-03-10 23:17:36	0d 0h 3m 17s	1/4 SSH OK - OpenSSH_5.3 (protocol 2.0)
	Total Processes	OK	2015-03-10 23:18:46	0d 0h 7m 7s	1/4 PROCS OK: 125 processes
Linux_192.168.0.130	Current Load	OK	2015-03-10 23:18:58	0d 0h 19m 33s	1/4 OK - load average: 2.21, 2.10, 1.33
	Current Users	OK	2015-03-10 23:19:42	0d 0h 18m 49s	1/4 USERS OK - 1 users currently logged in
	Disk Space	OK	2015-03-10 23:20:26	0d 0h 18m 5s	1/4 DISK OK
	HTTP	CRITICAL	2015-03-10 23:18:10	0d 0h 17m 21s	4/4 Connection refused
	PING	OK	2015-03-10 23:18:10	0d 0h 16m 37s	1/4 PING OK - Packet loss = 0%, RTA = 5.82 ms
	SSH	OK	2015-03-10 23:17:38	0d 0h 3m 15s	1/4 SSH OK - OpenSSH_6.1p1 Debian-4 (protocol 2.0)
	Total Processes	OK	2015-03-10 23:19:30	0d 0h 6m 23s	1/4 PROCS OK: 128 processes
Wind_192.168.0.1	Current Load	OK	2015-03-10 23:19:01	0d 0h 21m 17s	1/4 OK - load average: 2.21, 2.10, 1.33
	Current Users	OK	2015-03-10 23:19:45	0d 0h 20m 32s	1/4 USERS OK - 1 users currently logged in
	Disk Space	OK	2015-03-10 23:20:29	0d 0h 19m 48s	1/4 DISK OK
	HTTP	OK	2015-03-10 23:16:13	0d 0h 19m 3s	1/4 HTTP OK: HTTP/1.0 302 Redirect - 384 bytes in 0.008 second response time
	PING	OK	2015-03-10 23:16:57	0d 0h 18m 19s	1/4 PING OK - Packet loss = 0%, RTA = 1.53 ms
	SSH	CRITICAL	2015-03-10 23:19:10	0d 0h 17m 35s	4/4 Connection refused
	Total Processes	OK	2015-03-10 23:20:14	0d 0h 16m 50s	1/4 PROCS OK: 133 processes
Windows_192.168.0.101	Current Load	OK	2015-03-10 23:19:04	0d 0h 21m 13s	1/4 OK - load average: 2.03, 2.06, 1.33
	Current Users	OK	2015-03-10 23:19:48	0d 0h 20m 29s	1/4 USERS OK - 1 users currently logged in
	Disk Space	OK	2015-03-10 23:20:32	0d 0h 19m 44s	1/4 DISK OK
	HTTP	CRITICAL	2015-03-10 23:16:16	0d 0h 19m 0s	4/4 Connection refused
	PING	OK	2015-03-10 23:17:00	0d 0h 18m 15s	1/4 PING OK - Packet loss = 0%, RTA = 2.05 ms
	SSH	CRITICAL	2015-03-10 23:19:10	0d 0h 17m 31s	4/4 Connection refused
	Total Processes	OK	2015-03-10 23:15:58	0d 0h 16m 46s	1/4 PROCS OK: 121 processes

Figura. Equipos en la consola NAGIOS, ejecutando el Gestor.
Elaborado por: Diego Poveda & Alexis Balarezo

Para la verificación de los tiempos de creación del Gestor de host NAGIOS se ejecuta el desarrollado script tiempo.sh el cual fue elaborado para ejecutarse internamente con el Gestor o en forma manual.

Verificación de tiempo de ejecución

```
192.168.0.110 activo
Equipo ya registrado

192.168.0.111 activo
Equipo ya registrado

192.168.0.113 pasivo
192.168.0.114 activo
Equipo ya registrado

192.168.0.115 activo
Equipo ya registrado

192.168.0.117 pasivo
192.168.0.118 activo
Equipo ya registrado

192.168.0.119 pasivo
192.168.0.120 activo
Equipo ya registrado

192.168.0.129 pasivo
192.168.0.130 activo
Equipo ya registrado

192.168.0.209 pasivo
Restarting nagios3 monitoring daemon: nagios3Waiting for nagios3 daemon to die...
.
escaneo completo
Tiempo de ejecución: 34.20 segundos
```

Figura. Ejecución del script timepo.sh
Elaborado por: Diego Poveda & Alexis Balarezo

Anexo 5. Pruebas OSSEC optimización de tiempos

- **Pruebas eventos OSSEC pre-implementación**

En las siguientes figuras se muestra el resultado de las pruebas realizadas mediante el acceso remoto al host por medio de SSH para la generación de eventos OSSEC sin haber realizado cambios en la herramienta, donde se observa la variación de tiempo entre la suscitación del evento y la visualización del mismo en la consola administrativa.

Autenticación correcta mediante SSH

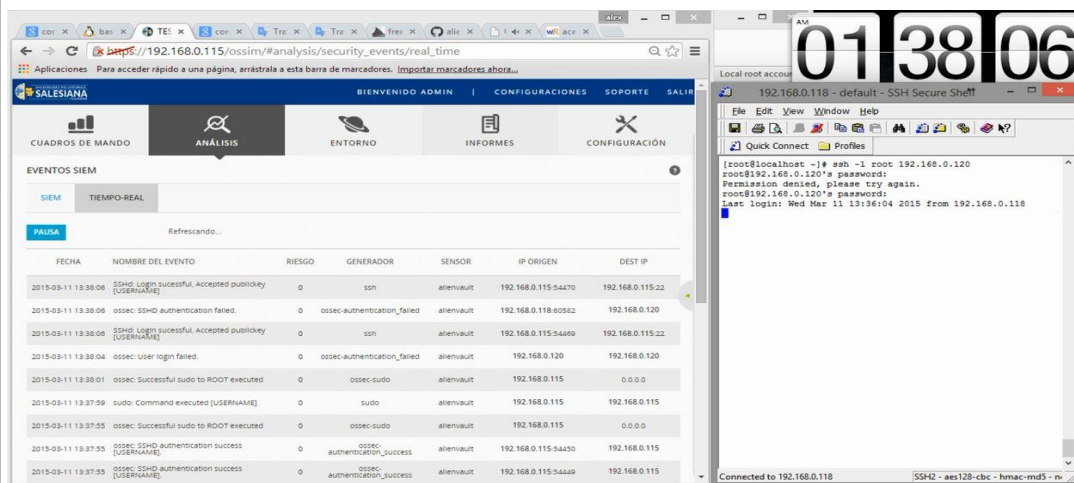


Figura. Autenticación SSH correcta a host pre-implementación
Elaborado por: Diego Poveda & Alexis Balarezo

Visualización de evento consola administrativa

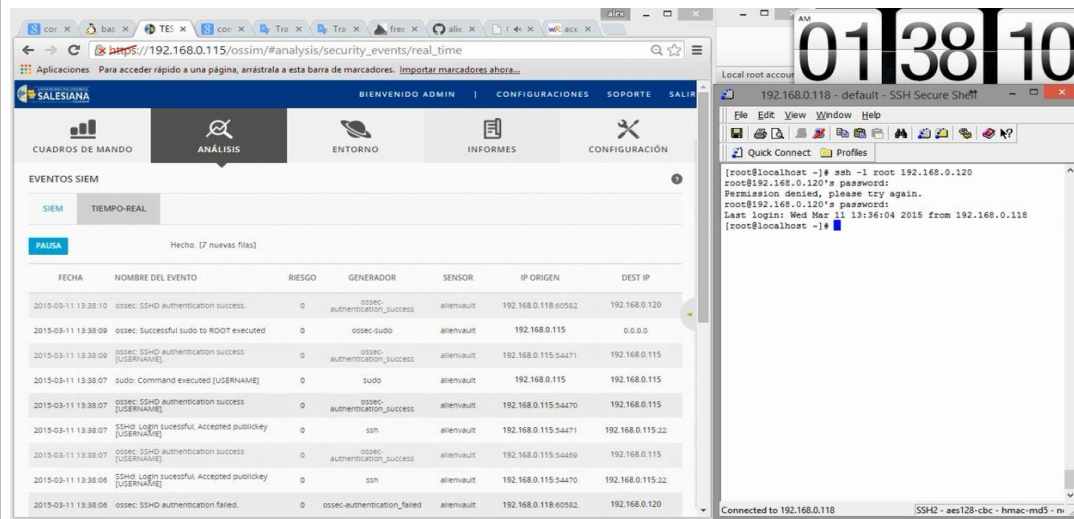


Figura. Autenticación SSH correcta a host pre-implementación
Elaborado por: Diego Poveda & Alexis Balarezo

Autenticación incorrecta mediante SSH

The screenshot shows a web application interface for 'SALESIANA' with a navigation bar and a main content area. The 'ANÁLISIS' tab is selected, displaying a table of security events. To the right, an SSH terminal window is open, showing a series of failed login attempts for the 'root' user on host 192.168.0.120.

FECHA	NOMBRE DEL EVENTO	RIESGO	GENERADOR	SENSOR	IP ORIGEN	DEST IP
2015-03-11 11:07:54	ossec: successful sudo to ROOT executed	0	ossec-sudo	alienVault	192.168.0.115	0.0.0.0
2015-03-11 11:07:54	ossec: SSH authentication success [USERNAME]	0	ossec-authentication_success	alienVault	192.168.0.115:60423	192.168.0.115
2015-03-11 11:07:54	ossec: SSH authentication success [USERNAME]	0	ossec-authentication_success	alienVault	192.168.0.115:60422	192.168.0.115
2015-03-11 11:07:54	ossec: SSH authentication success [USERNAME]	0	ossec-authentication_success	alienVault	192.168.0.115:60421	192.168.0.115
2015-03-11 11:07:54	sudo: Command executed [USERNAME]	0	sudo	alienVault	192.168.0.115	192.168.0.115
2015-03-11 11:07:54	SSHd: Login successful: Accepted publickey [USERNAME]	0	sshd	alienVault	192.168.0.115:60423	192.168.0.115:22
2015-03-11 11:07:53	SSHd: Login successful: Accepted publickey [USERNAME]	0	sshd	alienVault	192.168.0.115:60422	192.168.0.115:22
2015-03-11 11:07:53	SSHd: Login successful: Accepted publickey [USERNAME]	0	sshd	alienVault	192.168.0.115:60421	192.168.0.115:22
2015-03-11 11:07:48	ossec: successful sudo to ROOT executed	0	ossec-sudo	alienVault	192.168.0.115	0.0.0.0

```
[root@localhost ~]# ssh -l root 192.168.0.120
root@192.168.0.120's password:
Permission denied, please try again.
root@192.168.0.120's password:
Permission denied, please try again.
root@192.168.0.120's password:
Permission denied, please try again.
root@192.168.0.120's password:
Connection closed by 192.168.0.120
[root@localhost ~]# ssh -l root 192.168.0.120
root@192.168.0.120's password:
Permission denied, please try again.
root@192.168.0.120's password:
Permission denied, please try again.
root@192.168.0.120's password:
Permission denied, please try again.
root@192.168.0.120's password:
Permission denied, please try again.
root@192.168.0.120's password:
Last login: Wed Mar 11 10:31:07 2015 from 192.168.0.118
[root@localhost ~]# exit
logout
Connection to 192.168.0.120 closed.
[root@localhost ~]# ssh -l root 192.168.0.120
root@192.168.0.120's password:
Permission denied, please try again.
root@192.168.0.120's password:
Permission denied, please try again.
root@192.168.0.120's password:
Permission denied, please try again.
root@192.168.0.120's password:
Last login: Wed Mar 11 11:05:28 2015 from 192.168.0.118
[root@localhost ~]# exit
logout
Connection to 192.168.0.120 closed.
[root@localhost ~]# ssh -l root 192.168.0.120
root@192.168.0.120's password:
Permission denied, please try again.
root@192.168.0.120's password:
Permission denied, please try again.
root@192.168.0.120's password:
Permission denied, please try again.
root@192.168.0.120's password:
Connection closed by 192.168.0.120
[root@localhost ~]#
```

Figura. Autenticación SSH incorrecta a host pre-implementación

Elaborado por: Diego Poveda & Alexis Balarezo

Visualización de evento consola administrativa

The screenshot shows the same web application interface as before, but the 'EVENTOS SIEM' table now includes a new entry for a failed login attempt. The SSH terminal window on the right shows a successful login for the 'root' user on host 192.168.0.120.

FECHA	NOMBRE DEL EVENTO	RIESGO	GENERADOR	SENSOR	IP ORIGEN	DEST IP
2015-03-11 11:07:56	ossec: User login failed.	0	ossec-authentication_failed	alienVault	192.168.0.120	192.168.0.120
2015-03-11 11:07:54	ossec: successful sudo to ROOT executed	0	ossec-sudo	alienVault	192.168.0.115	0.0.0.0
2015-03-11 11:07:54	ossec: SSH authentication success [USERNAME]	0	ossec-authentication_success	alienVault	192.168.0.115:60423	192.168.0.115
2015-03-11 11:07:54	ossec: SSH authentication success [USERNAME]	0	ossec-authentication_success	alienVault	192.168.0.115:60422	192.168.0.115
2015-03-11 11:07:54	ossec: SSH authentication success [USERNAME]	0	ossec-authentication_success	alienVault	192.168.0.115:60421	192.168.0.115
2015-03-11 11:07:54	sudo: Command executed [USERNAME]	0	sudo	alienVault	192.168.0.115	192.168.0.115
2015-03-11 11:07:54	SSHd: Login successful: Accepted publickey [USERNAME]	0	sshd	alienVault	192.168.0.115:60423	192.168.0.115:22
2015-03-11 11:07:53	SSHd: Login successful: Accepted publickey [USERNAME]	0	sshd	alienVault	192.168.0.115:60422	192.168.0.115:22
2015-03-11 11:07:53	SSHd: Login successful: Accepted publickey [USERNAME]	0	sshd	alienVault	192.168.0.115:60421	192.168.0.115:22

```
[root@localhost ~]# ssh -l root 192.168.0.120
root@192.168.0.120's password:
Permission denied, please try again.
root@192.168.0.120's password:
Permission denied, please try again.
root@192.168.0.120's password:
Permission denied, please try again.
root@192.168.0.120's password:
Permission denied, please try again.
root@192.168.0.120's password:
Connection closed by 192.168.0.120
[root@localhost ~]# ssh -l root 192.168.0.120
root@192.168.0.120's password:
Permission denied, please try again.
root@192.168.0.120's password:
Permission denied, please try again.
root@192.168.0.120's password:
Permission denied, please try again.
root@192.168.0.120's password:
Permission denied, please try again.
root@192.168.0.120's password:
Last login: Wed Mar 11 10:31:07 2015 from 192.168.0.118
[root@localhost ~]# exit
logout
Connection to 192.168.0.120 closed.
[root@localhost ~]# ssh -l root 192.168.0.120
root@192.168.0.120's password:
Permission denied, please try again.
root@192.168.0.120's password:
Permission denied, please try again.
root@192.168.0.120's password:
Permission denied, please try again.
root@192.168.0.120's password:
Connection closed by 192.168.0.120
[root@localhost ~]#
```

Figura. Visualización autenticación SSH incorrecta a host pre-implementación

Elaborado por: Diego Poveda & Alexis Balarezo

- **Pruebas eventos OSSEC post-implementación**

En las siguientes figuras se muestra el resultado de las pruebas realizadas mediante el acceso remoto al host por medio de SSH para la generación de eventos OSSEC una vez realizado los cambios en la herramienta, donde se observa la variación de tiempo entre la suscitación del evento y la visualización del mismo en la consola administrativa, haciendo notoria la disminución de periodo de respuesta.

Autenticación correcta mediante SSH con visualización inmediata

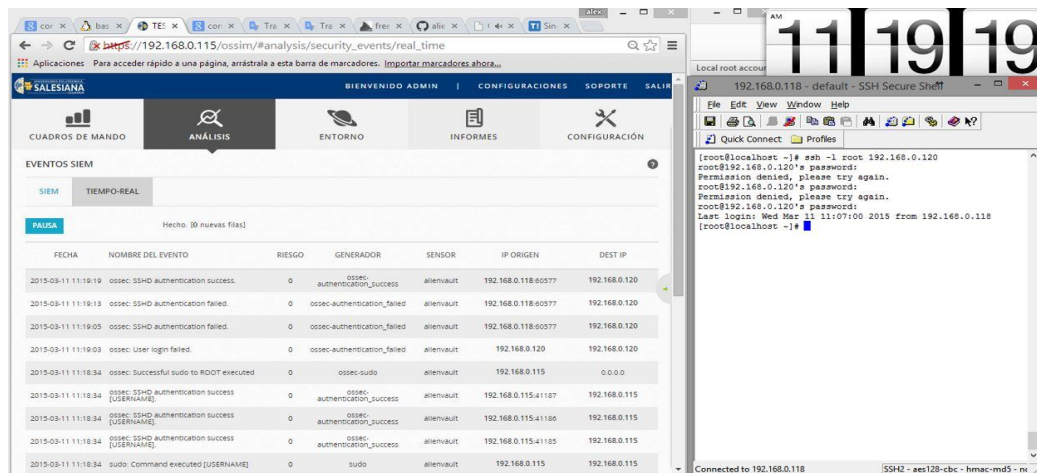


Figura. Visualización autenticación SSH correcta a host post-implementación
Elaborado por: Diego Poveda & Alexis Balarezo

Autenticación incorrecta mediante SSH con visualización inmediata

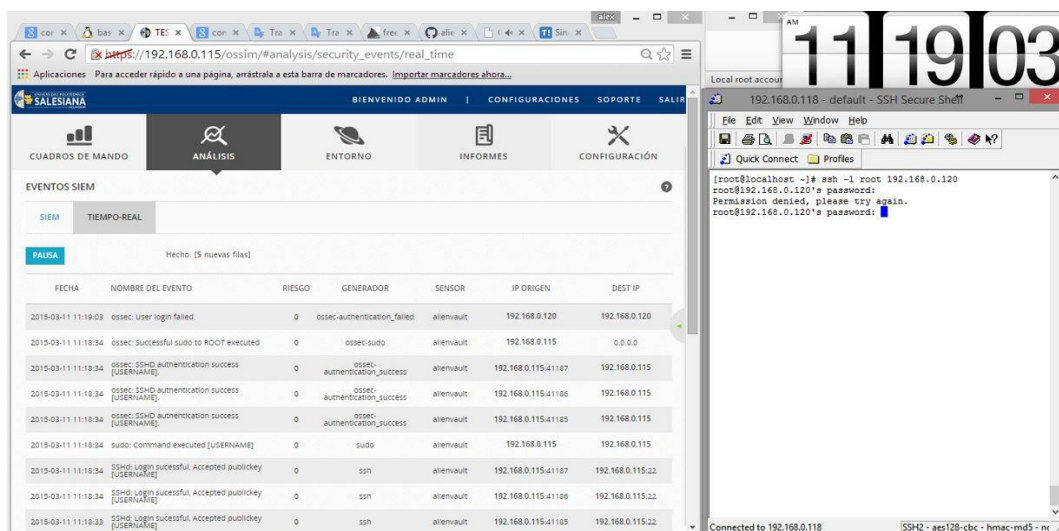


Figura. Visualización autenticación SSH incorrecta a host post-implementación
Elaborado por: Diego Poveda & Alexis Balarezo